ecora

Ecora Patch Manager 4.0

User Manual

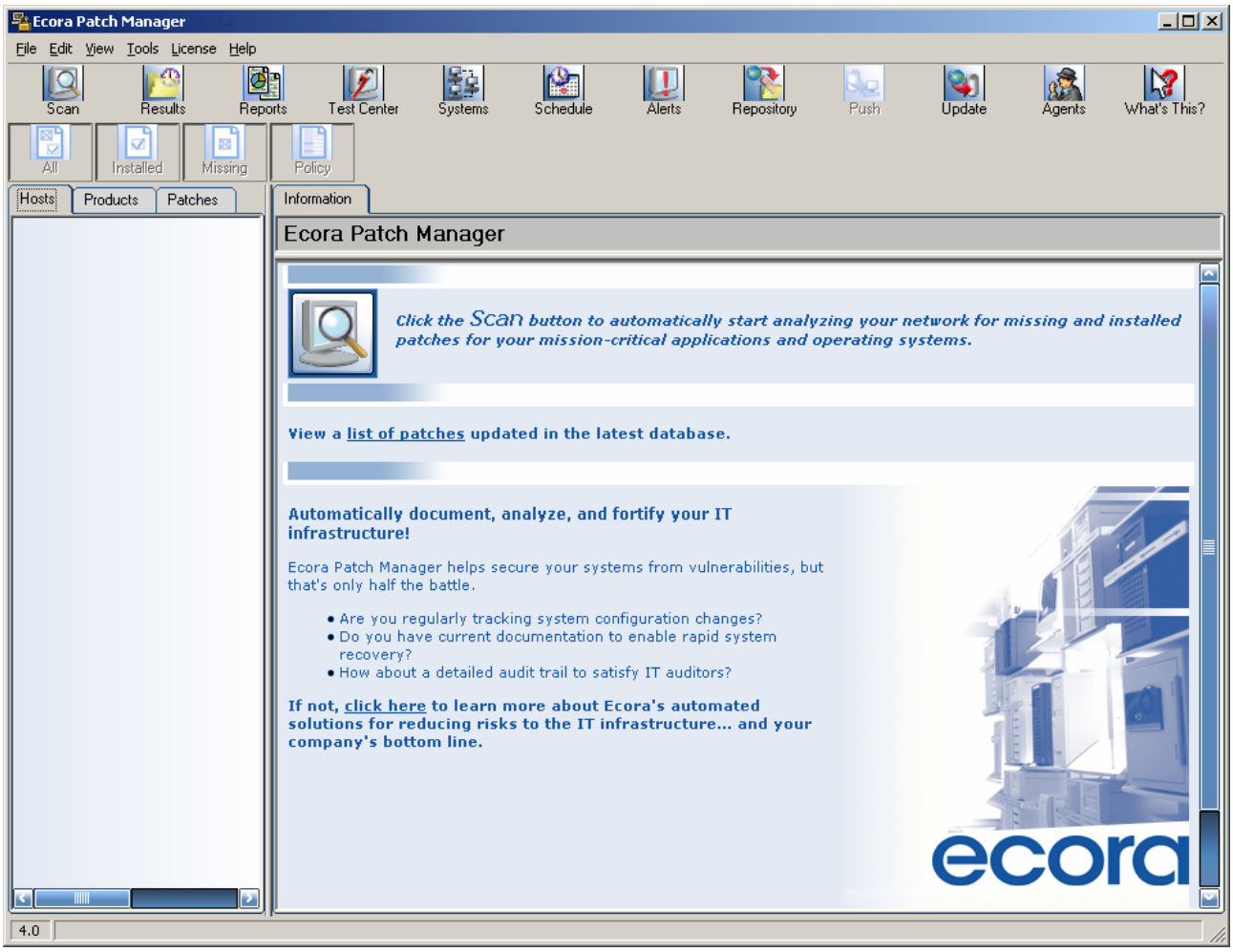
Table of Contents

Install the Software 3
User Interface Overview 4
    Main Window 4
    Button Bar 5
    Menu Bar 6
Settings & Preferences 8
Analyzing the Network 15
Discovering Systems 16
    Discovering Windows Systems 16
    Specifying Unix Systems 19
Managing Systems & Groups 22
    System & Group Properties 23
Understanding Scans 26
    Analysis Icons 27
Saving Scans 29
Installing Patches & Hotfixes 30
Using Rollback 30
Push & Rollback Jobs 31
    Job Settings 31
    User Delay 33
Patch Repository Management 34
    Patch Repository Maintenance 35
Patch Notes & Properties 37
Scheduling Patch Analysis 40
    Scheduling Scans 40
    Windows Task Scheduler 41
Getting Updates 42
    Scheduling Updates 42
    Migrating the Database 43
Agent Installation & Setup 44
    Installing the Agent Manager 44
    Installing Agents 45
Agent Management 47
    Agent Manager Console 48
    Scheduling Analysis for Agents 49
Using Alerts & Triggers 50
Policy Management 54
    Creating Policies 54
    Applying Policies to Systems and Groups 56
    Viewing by Policy Compliance 57
    Remediation by Policy 57
Patch Test Center 58
Reporting Center 60
    Installing the Reporting Center 60
    Using the Reporting Center 61
    Administering the Reporting Center 63
Troubleshooting 65
Ecora Copyright Notice 66

Install the Software

Please refer to the **Patch Manager 4.0 Start-up Guide**, located on Ecora's Support webpage (http://www.ecora.com/ecora/support/pm4startup-guide.pdf) for instructions on how to download, install, and configure Ecora Patch Manager Version 4.0.

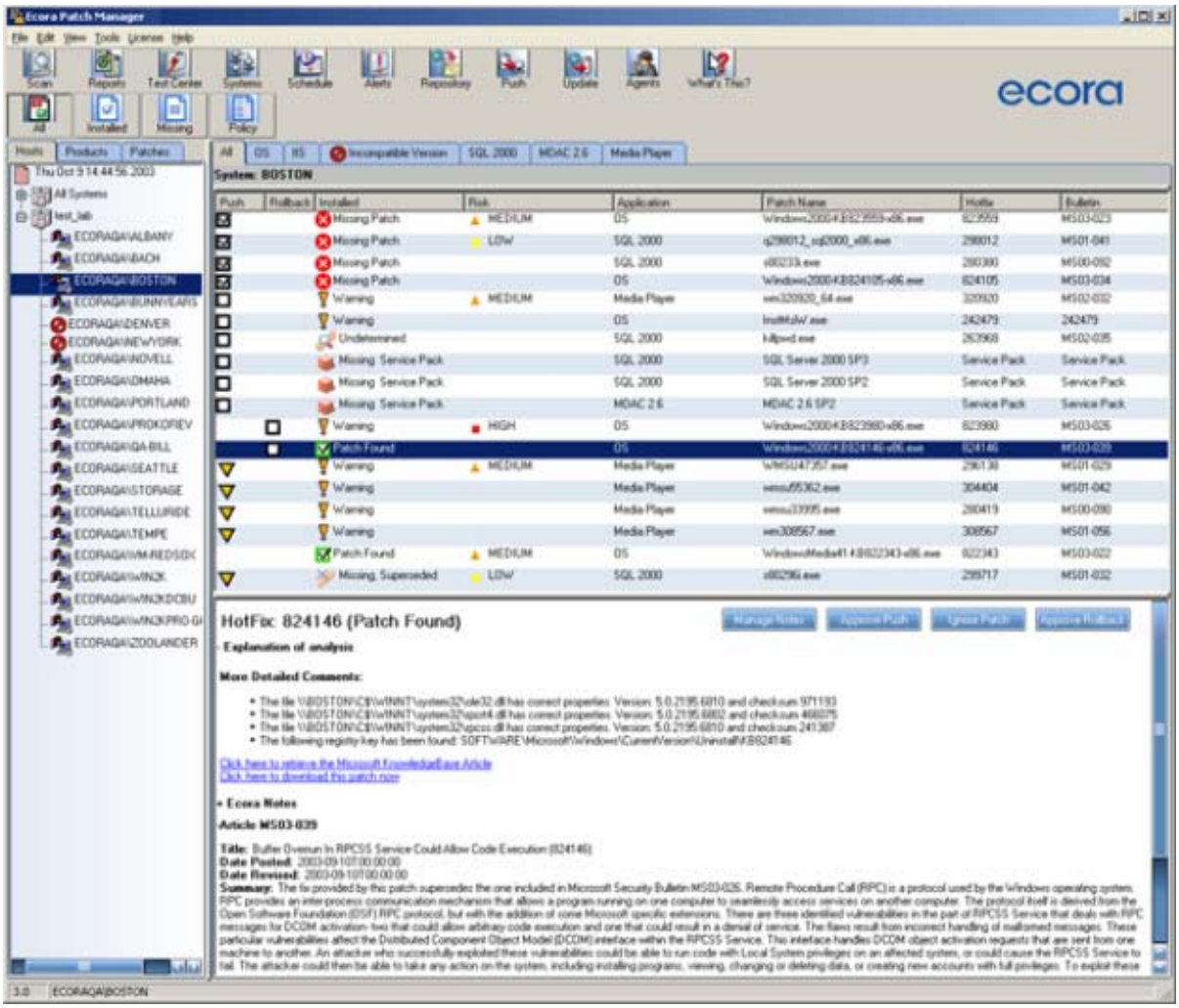
You should be here…


Ecora Patch Manager
File Edit View Tools License Help
Scan
Results
Reports
Test Center
Systems
Schedule
Alerts
Repository
Push
Update
Agents
What's This?
All
Installed
Missing
Policy
Hosts
Products
Patches
Information
Ecora Patch Manager
Click the Scan button to automatically start analyzing your network for missing and installed patches for your mission-critical applications and operating systems.
View a list of patches updated in the latest database.
Automatically document, analyze, and fortify your IT infrastructure!
Ecora Patch Manager helps secure your systems from vulnerabilities, but that's only half the battle.
• Are you regularly tracking system configuration changes?
• Do you have current documentation to enable rapid system recovery?
• How about a detailed audit trail to satisfy IT auditors?
If not, click here to learn more about Ecora's automated solutions for reducing risks to the IT infrastructure... and your company's bottom line.
ecora
4.0

User Interface Overview

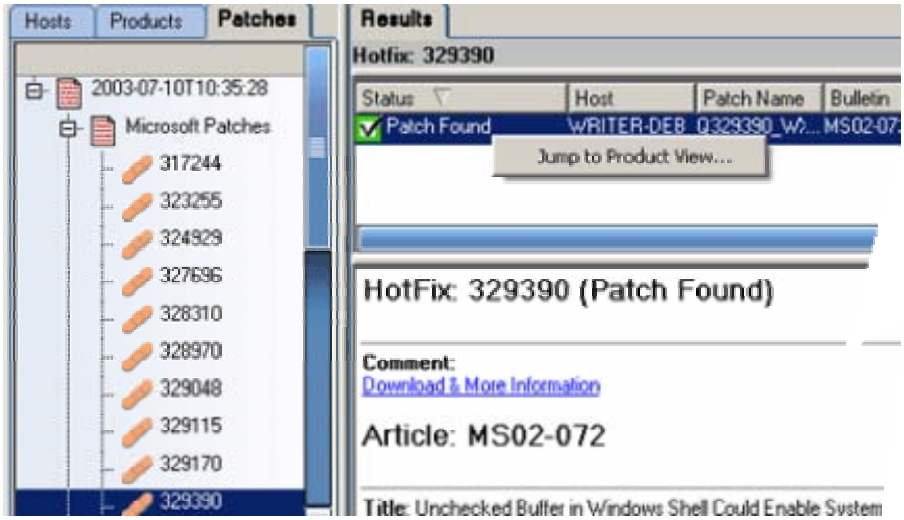
Main Window

The toolbar is divided into two bars: **Tasks** and **Views**. The upper task buttons perform actions whereas the lower view button change or filter the display of the current analysis.



The left window pane contains three tabs that allow you to choose how you wish to organize your analysis.
The **Hosts** tab displays the data and network structure, allowing you to drill down (expanding on the plus signs) through reports, OS, and domains to systems.
The **Products** tab displays supported items for patch analysis, such as OS, IIS, SQL.
The **Patches** tab displays all relevant patches and service packs in numerical order.
The **Policy** tab displays all policies relevant to the selected scan (available only with the Policy view is active).

Right-clicking is the method for "drilling down" to additional detail in the report. Right-click on any item to see if a "Jump to view..." is available for related information.



The upper right window pane displays the patches relevant to the selection in the left pane and applicable to the active tab above. It provides sortable columns of patch data, check boxes for selecting patches for **Push** (installation) and **Rollback** (un-installation). Click in a checkbox to select that patch for installation (push) or un-installation (rollback).

The lower right window pane contains details of the selected patch, including download links, related articles, Ecora Notes, and buttons for you to **Manage Notes**, **Ignore Patch**, **Approve Push**, and **Approve Rollback**.

Button Bar

Scan - Begins the process of analyzing the network for patch versions.

Results - Accesses a dialog box in which to load analysis results from past scans *(see Saving Scans)*.

Reports - Accesses the online Reporting Center - a webpage for querying patch analysis results and creating reports *(see Reporting Center)*.

Test Center - Accesses the interface for selecting systems to act as test machines on which patches and hotfixes are installed prior to deployment on production systems *(see Test Center)*.

Systems - Accesses the dialog box in which to group systems, set system credentials, and discover new systems *(see Grouping Systems)*.

Schedule - Accesses a dialog box in which to enable and schedule automatic analysis *(see Scheduling)*.

Alerts - Accesses a dialog box in which to create or modify checks notifications by the software when user-defined conditions are met *(for details, see Alerting)*.

Repository - Accesses the dialog box in which to manage patch repositories, archives of downloaded patches *(see Patch Repository Management)*.

Push - Accesses the dialog box in which to manage patch installation, including installation time, grouping, and reboot options *(see Installing Patches)*.

Update - Updates the software or database with the latest from Ecora's website *(see Getting Updates)*.

Agents - Accesses the dialog box in which to manage agents; which systems have agents, how often agent systems will be scanned, and other settings. *(see Optional Agent)*.

What's This - Accesses a brief explanation of the next item clicked in the user interface.

All - Displays all service packs, hotfixes, notes, and warnings for both installed and not installed patches applicable the selected system.

Installed - Displays all available and compatible patches detected as installed.

Missing - Displays all compatible patches for the selected system detected as not installed.

Policy - Displays patches and systems according to compliance with user-defined policies *(see Using Policies)*.

Menu Bar

File...

New Scan... begins the process of analyzing the network for patch versions.
Open Scan Results... accesses a dialog box in which to locate and open a saved scan report.
Settings... accesses a dialog box in which to set the user preferences.
Update... accesses the Ecora website page to find available downloads/updates for the software or patch database.
Import Scan... accesses a dialog box in which to locate and open a saved scan analysis.
Export Scan... accesses a dialog box in which to name and write the current analysis to disk.
Exit closes the application.

Edit...

Alerts and Triggers... accesses a dialog box in which to create or modify notifications by the software when user-defined conditions are met *(for details, see Alerting)*.

View...

All Patches displays the service packs, hotfixes, notes, and warnings for both installed and not installed patches applicable to the selected system. The report is a list of both current packages and ones that have been superseded.
Installed Patches displays all available patches applicable to the selected system that were detected as installed.
Missing Patches displays all available patches applicable to the selected system that were

not detected as installed.
Policy displays all patches and systems according to compliance with user-defined policies.
View Log... displays the record of patch deployment (date, session ID, severity, system upgraded, etc.) in an HTML file. The log may contain a link to the log file of the target system(s), where details of the patch installation are recorded.

Tools...

Systems Grouping... accesses the dialog box in which to group systems, set system credentials, and discover new systems.
Agents... accesses the dialog box in which to schedule agent scans, change agents settings, etc. *(for details, see Agent Management).*
Policy Management... accesses the dialog box in which to define and edit policies *(for details, see Policy Management).*
Policy Selection... accesses the dialog box in which to apply policies to systems or groups of systems.
Repository Management... accesses the dialog box in which to define repository locations and maintenance schedules *(for details, see Repository Management).*
Custom Notes Management... accesses the dialog box in which hide patches, approve patches, and add your and comments to patches *(for details, see Custom Notes Management).*
Push Patches... accesses the dialog box in which to manage patch installation, including installation time, grouping, and reboot options.
Schedule Updates... accesses the dialog box in which to enable and schedule automatic checking for and/or downloading a new patch database.
Schedule Scans... accesses a dialog box in which to enable and schedule automatic analysis.
Test Center... accesses a dialog box in which to locate or create a system to be used for the purposes of testing patches prior to deploying in production.
Reporting Center... accesses the online reporting center where the patch knowledge base can be queried.

License...

View License... accesses a dialog box that displays the license data associated with this software, including number of systems licensed.
Update License... accesses a dialog box in which to provide a unique license key to enable the software.
Purchase License... accesses a dialog box in which the software product ID can be mailed to Ecora to purchase a license.

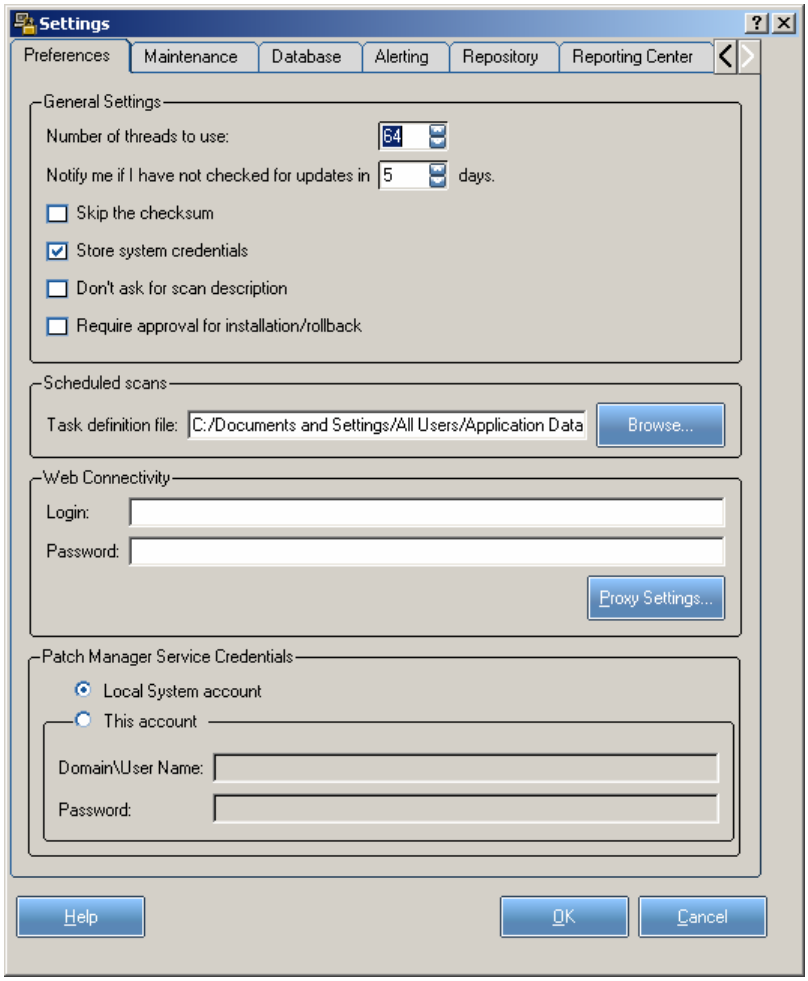
Help...

Help Topics... accesses the online user manual pages.
About... accesses a dialog box that presents the versions of each component of the software.
What's This? enables the on-screen, pop-up help for the next item clicked.

Settings & Preferences

You have the ability to customize your global settings and preferences, including the data source, alerting setup, number of threads used, and the output formats for reports.

To change the settings:



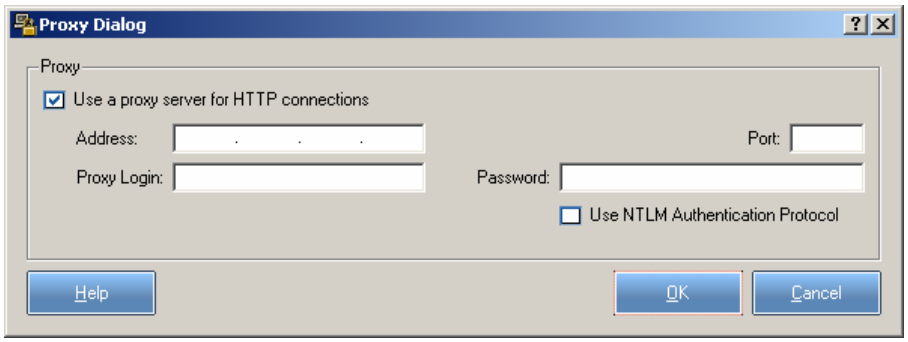
1. Choose **File... Settings...** from the menu.
2. On the **Preferences** tab, accept or change the number of threads (simultaneous connections) being used to analyze the network.
3. Accept or change the number of number of days you consider an acceptable age for the patch database before being warned that the data is old. You can also choose to schedule updates.
4. Click in the **Skip the checksums** checkbox if you wish to disable the checksum matching that is used in patch analysis to verify the patches are correctly installed.
5. Click in the **Store system credentials** checkbox if you wish to save login and passwords, encrypted, to disk for repeated use.
   Note: Saved credentials are used for scanning, pushing, repository connections, updates, and scheduling. Disabling this option will limit the software functionality considerably.
6. Click in the **Don't ask for scan description** checkbox if you wish to name by default vs prompting during each scan.
7. Click in the **Require approval for installation / rollback** checkbox if you wish to enable approving patches for push or rollback.
8. Accept the default or specify path to (or use the **Browse...** button to locate) task definition files (used for any scheduled scan, push, or rollback).
9. Enter your Ecora website username and password (for software upgrades and licensing).

10. If a proxy server or non-standard port is used to access the Internet, click on the **Proxy Settings...** button.

    A. Click in the checkbox for the **Use a proxy server for HTTP connections** option.

    B. Enter the IP Address.

    C. Enter the Port to be used.



    D. Enter a valid Proxy Login and Password to authenticate.

    E. Click in the checkbox for the **Use NTLM Authentication Protocol** option if your network is using this protocol.

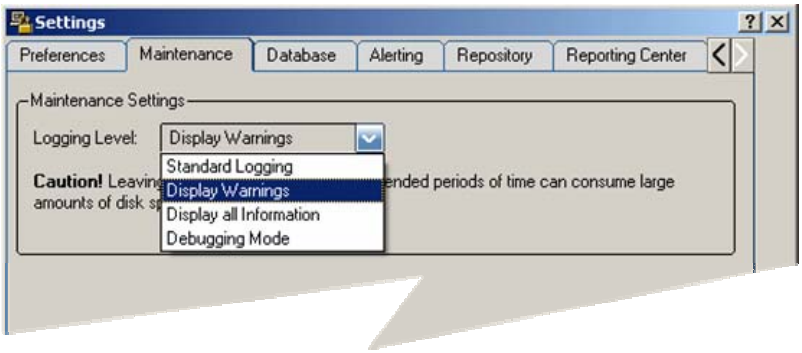
    F. Click **OK**.

11. In the Patch Manager Service Credentials area, enable either **Local System Account** or **This Account** for scheduling tasks, repository maintenance, and patch deployment.

12. If you chose to specify an account, enter a valid login and password for the Ecora Patch Service to use.

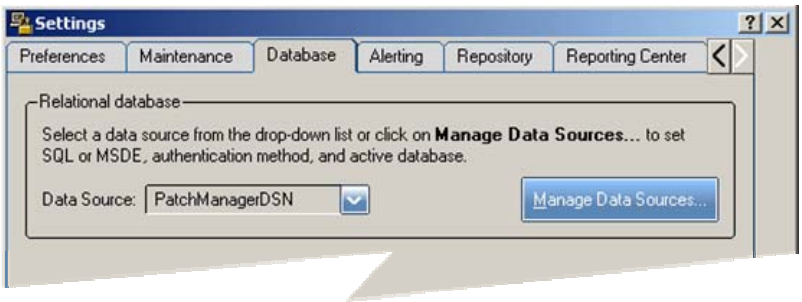
13. Click on the **Maintenance** tab.

14. Accept or change the logging level (higher for troubleshooting).

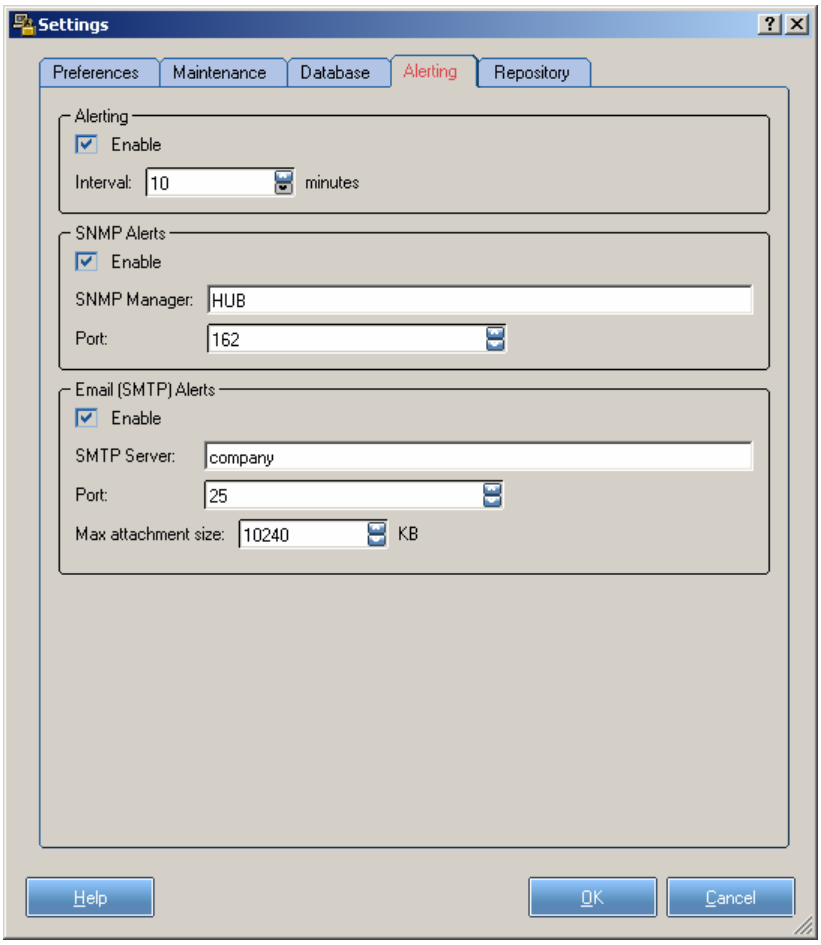


15. Click on the **Database** tab.

16. Choose an existing data source from the drop-down list or press the **Manage Data Sources** button to define one *(for details, see Database Setup)*.



17. Click on the **Alerting** tab.
18. In the Alerting area, click in the **Enable** checkbox to enable monitoring.
19. Use the drop-down list to select an interval (in minutes- minimum 10 minutes) to set how often the software checks for the conditions you define.
20. In the Service Log On area, either select **Local System Account** or to specify the **Account** and enter valid credentials.
21. In the SNMP Alerts area, click in the **Enable** checkbox to enable alerts via SNMP traps.
22. Enter the SNMP Manager name and Port number. The SNMP Manager can be the name of any server running an application capable of receiving SNMP traps.



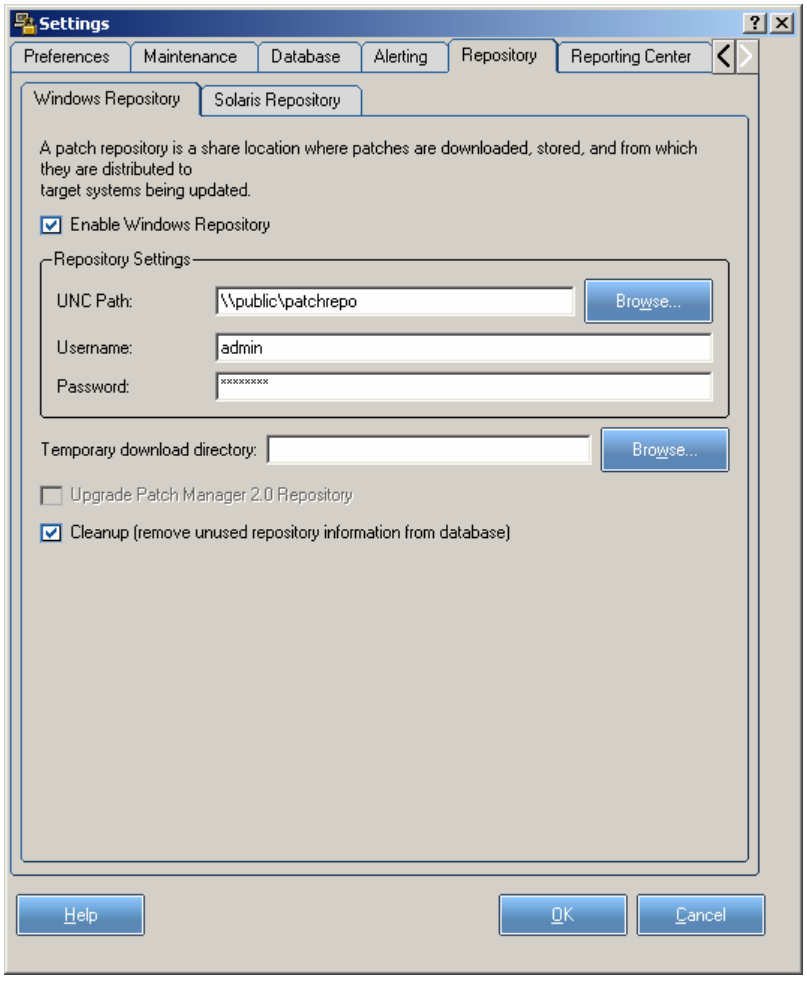
23. In the Email (SMTP) Alerts area, click in the **Enable** checkbox to enable alerts via email.

    Enter the SMTP Server name, Port number, and the Maximum Attachment Size (reports can get large). The SMTP Server is generally your mail server, such as mail.companyname.com.

    For additional information, see Using Alerts and Triggers.

    For additional information about SNMP, see Using SNMP for Network Management, Microsoft TechNet Chapter 11.

24. Click on the **Repository** tab.
25. Click on the **Windows** tab.
    26. Activate the checkbox to **Enable Windows Repository** for patch storage.
    27. Enter the path to the Windows patch repository or use the **Browse...** button to locate one (or a drive on which to create one).
        Tip: This must be share with a UNC path with "Uniform Naming Convention" such as \\ServerName\Share\Path. If you use the **Browse...** capability, remember to locate a local drive via its network share location, not via the local machine root. The result will be \\machinename\share vs c:\share.
    28. Enter a Username and Password (twice) with which to access the repository.



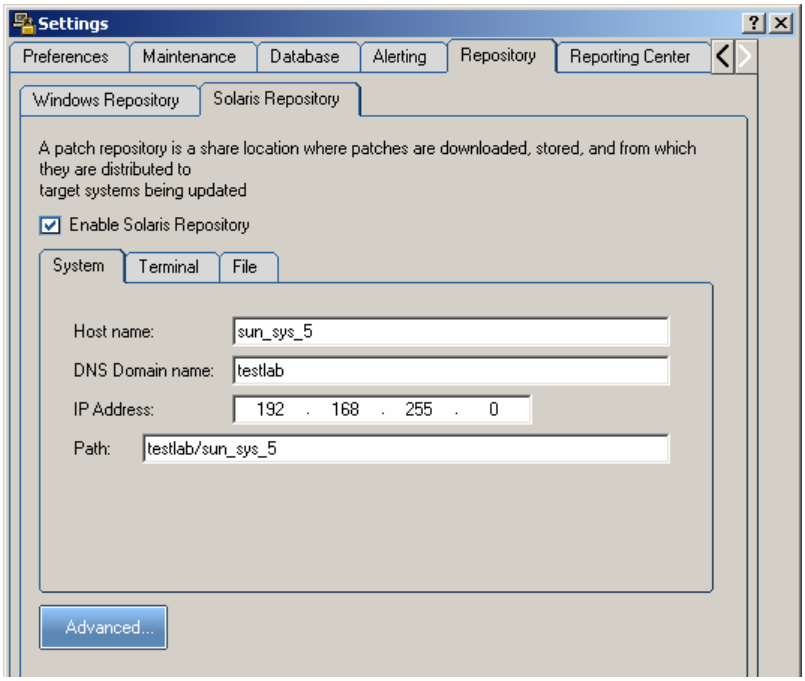
    29. If you wish, enter the path to the (local) temporary download directory where patches are downloaded and stored before being transferred to the repositories (via FTP for Unix and copied for Windows).
    30. If you wish, enable the **Upgrade** checkbox to migrate repository data from prior versions.
    31. If you wish, enable the **Cleanup** checkbox to have Patch Manager delete obsolete patch files.
    32. Enter the path to the (local) temporary download directory where patches are downloaded and stored before being transferred to the repositories (via FTP for Unix and copied for Windows).

33. If you are supporting Unix systems, click on the **Solaris Repository** tab.

34. Activate the checkbox to **Enable Solaris Repository** for patch storage.

35. Click on the **System** tab.

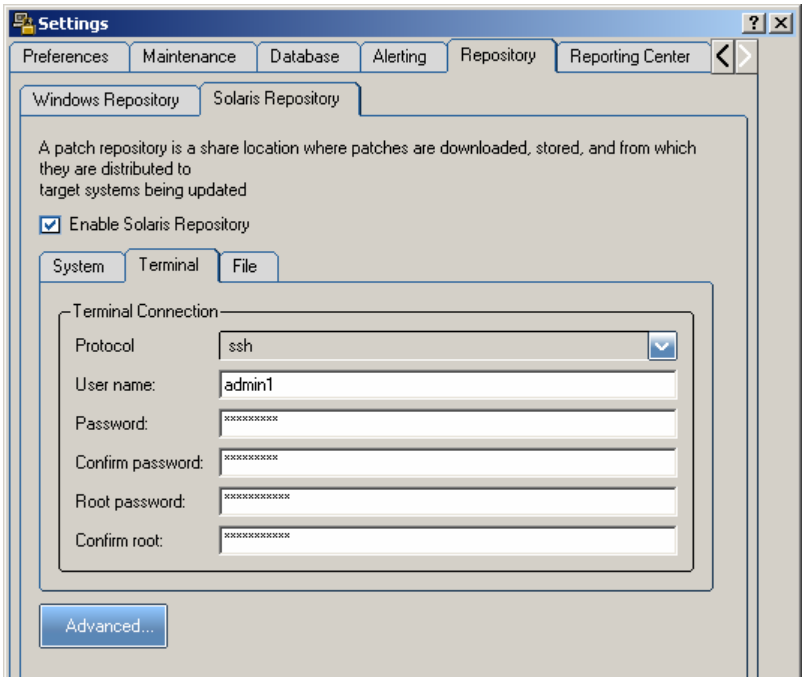
36. Enter the hostname, DNS Domain name, and/or IP Address of system housing the Unix patch repository.
    Tip: All three are not required - only the information necessary to resolve the system in your environment; perhaps only IP address, perhaps hostname and domain name.



37. Enter the Path to the Solaris patch repository.
    Note: Patch Manager validates the repository by creating a file in the directory that is later checked. Therefore, the directory (NSF mount path) must be mounted during system configuration for that file to be created.

38. Click on the **Terminal** tab.

39. Select a Protocol from the drop-down list.
    Read more about using SSH.



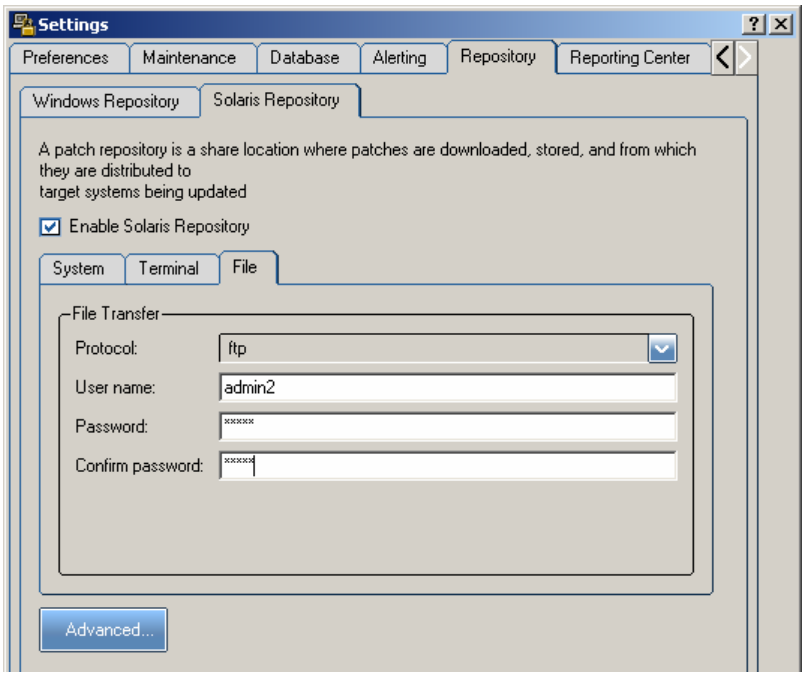
40. Enter a Username with which to connect to the repository.

41. Enter and confirm the Password for the user name.

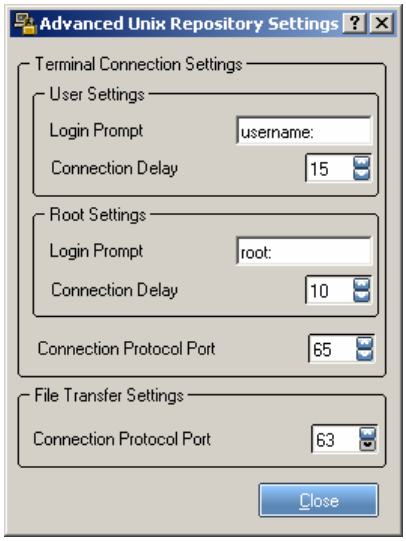
42. Enter the valid Root password for the system. To collect data beyond the areas the login user can access the root password for the target system is required.

43. Retype the root password to confirm that it's correct.
    Tip: The software can collect information to which the specified user account has

access. Additional system information can be gathered if the login user account is a member of group sys on the target systems. To enable the software to collect all configuration information root password is required.



44. Click on the **File** tab.
45. Select a Protocol from the drop-down list.
    Read more about using SSH.
46. Enter a Username with which to transfer files.
47. Enter and confirm the Password for the user name.
48. ONLY if you wish to change optional settings (such as using alternate ports), click the **Advanced...** button.



    A. Enter or select a Connection delay milliseconds. If supplied, the software waits this length of time after logging in before attempting to transmit anything to the target system.

    B. Enter the User login prompt for the repository. If supplied, the software waits for this text to appear on the connection before attempting to log into the system. If nothing is specified, it immediately attempts to login once the connection is established.

    C. Enter or select a Root connection delay in milliseconds. If supplied, the software waits this length of time after logging in before attempting to transmit anything to the target system.

    D. Enter the Root login prompt. If supplied, the software waits for this text to appear on the connection before attempting to log into the system. If nothing is specified, it immediately attempts to login once the connection is established.

    E. Specify the Connection Protocol Port number for terminal connections (0 uses the default for the selected protocol).

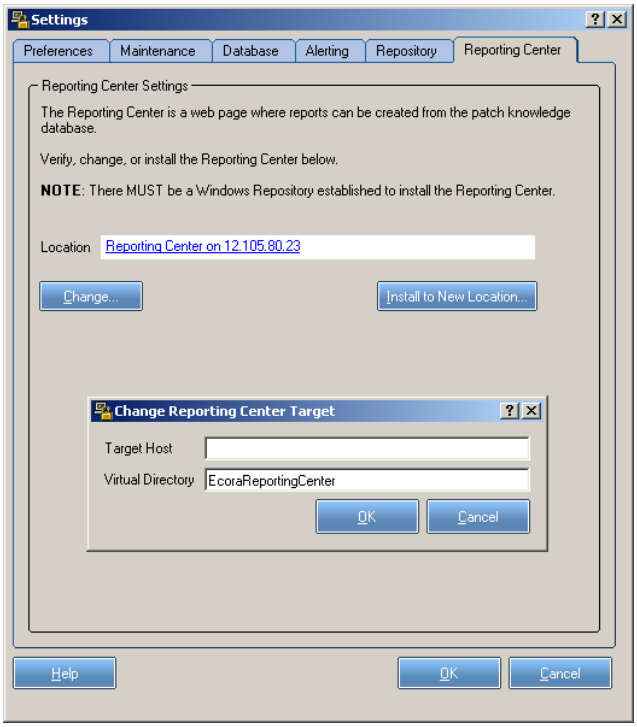
    F. Specify the Connection Protocol Port number for file transfers (0 uses the default for the selected protocol).

    Tips: Entering a ZERO (0) value for any advanced settings will use the defaults. A non-zero value in any of the connection delays will cause the software to delay that amount of time after a login (or after issuing the "su"

command in the case of root delay) before the software will execute any commands. The software follows the normal login procedure (send username, send password), then waits "n" milliseconds before returning "connection complete." A "non-zero" value in either of the prompt settings causes the software to, after the "normal" login procedure, search for the string entered as the users' prompt.

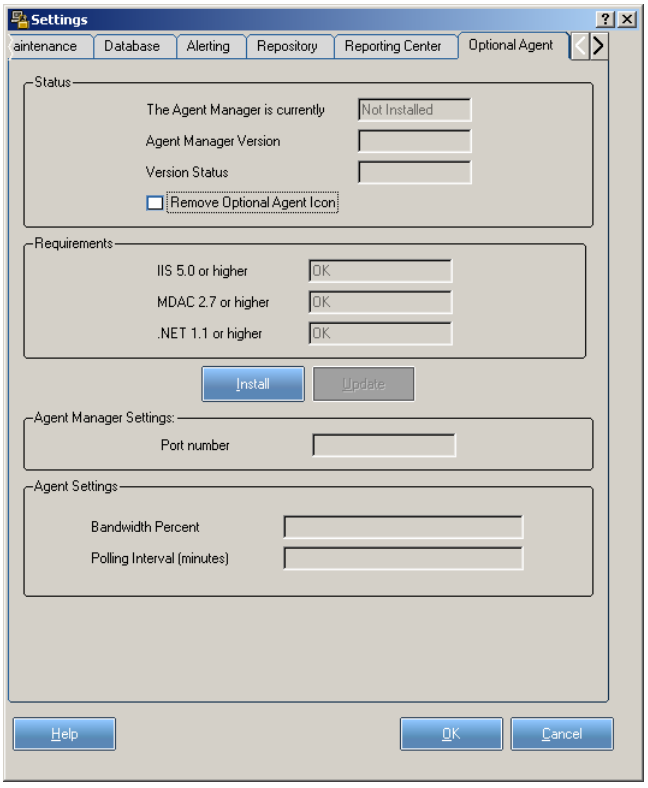
Read more about terminal connections.

49. Click on the **Reporting Center** tab.



50. Verify or access the current Reporting Center location.
51. Click on **Install to New Location...** to open the Reporting Center installation wizard and configure a Reporting Center.

    Note: There MUST be a Windows Repository established to install the Reporting Center.
52. Click on **Change...** to use a different Reporting Center installation that already exists. You'll be prompted for the new Target Host and Virtual Directory (where the Reporting Center is installed).
53. Click on the **Optional Agent** tab.
54. Verify the status of the Agent Manager; the version, the install state.
55. Enable the **Remove Optional Agent Icon** checkbox if you wish to delete the Agents button from the main toolbar.

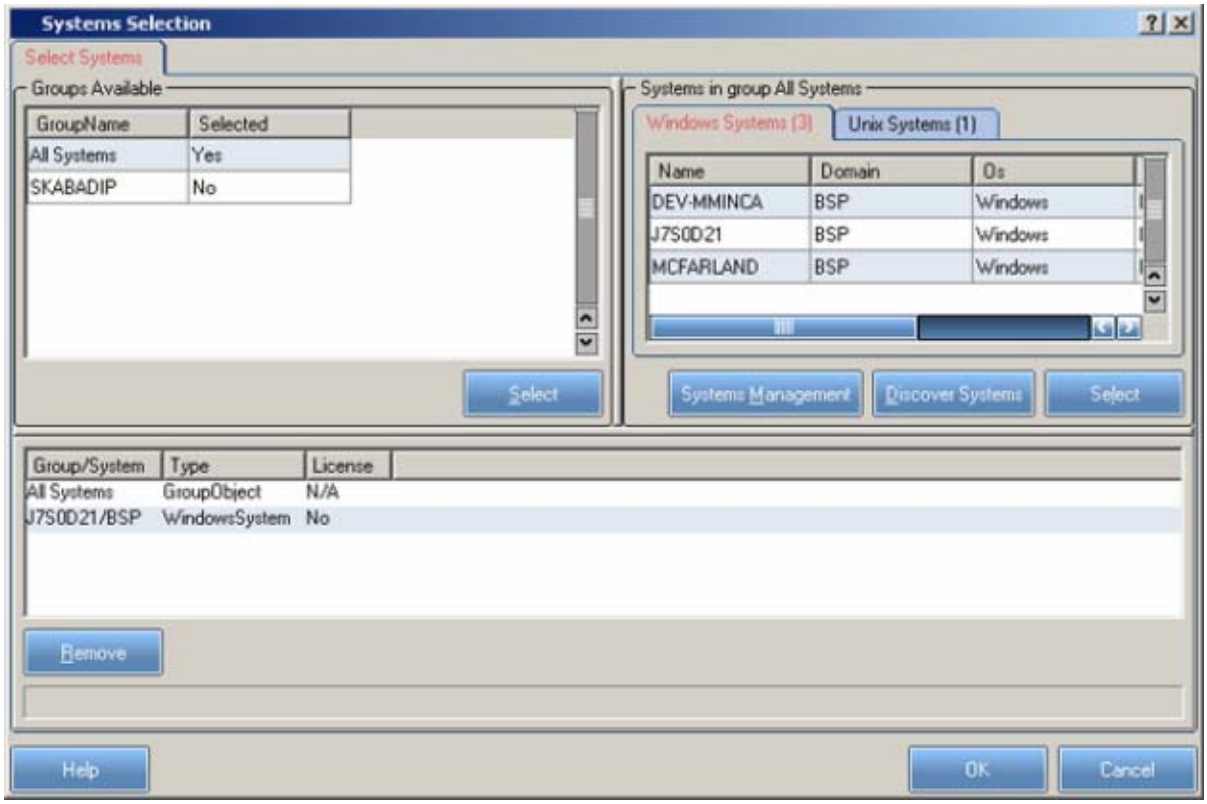


56. Verify the system requirements for Agent Manager are met; IIS 5.0, MDAC, .Net.
57. Click **Install...** to start the Agent Manager installation wizard and configure the port and bandwidth
    - OR -
    Click **Uninstall...** to start the Agent Manager uninstallation wizard to remove the Agent Manager.
58. Click on **Update...** to start the Agent Manager upgrade wizard for software updates.
59. Verify the **Port Number**, **Bandwidth Percent**, and **Polling Interval** (in minutes).
60. Click **OK**.

Analyzing the Network

1. Click on the **Scan** button.
2. The first time you run the software (or any time you choose), you must **Discover or Specify Systems** to scan.

   Tip: This first time you run version 3.0, you will be prompted to migrate any systems already discovered in version 2.0.
3. Select groups to scan from the Groups pane by highlighting them and using the **Select** button.
4. Select systems to scan from the Systems pane by highlighting them and using the **Select** button, using the **Windows** tab for Windows systems and the **Unix** tab for Unix systems.



5. If you wish to manage groups, click on the **Systems Management** button.
6. Verify that the systems you want analyzed all appear in the Selected Systems lower pane.
7. Click **OK** to begin scanning systems for patches.

   Note: Depending on the number of systems selected and the network configuration, this may take a few minutes.
   Clicking the **Stop** button will return results for any systems already scanned before the button is pressed.
8. If prompted, enter a scan description (for loading scan results at a later time).

9. After the scan has completed, the main window contains a tree view of systems reported in the left pane and information about the selected object in the right pane (see Understanding Scans).
10. If you wish to install patches, see push instructions.
11. If you wish to schedule scanning, see schedule instructions.

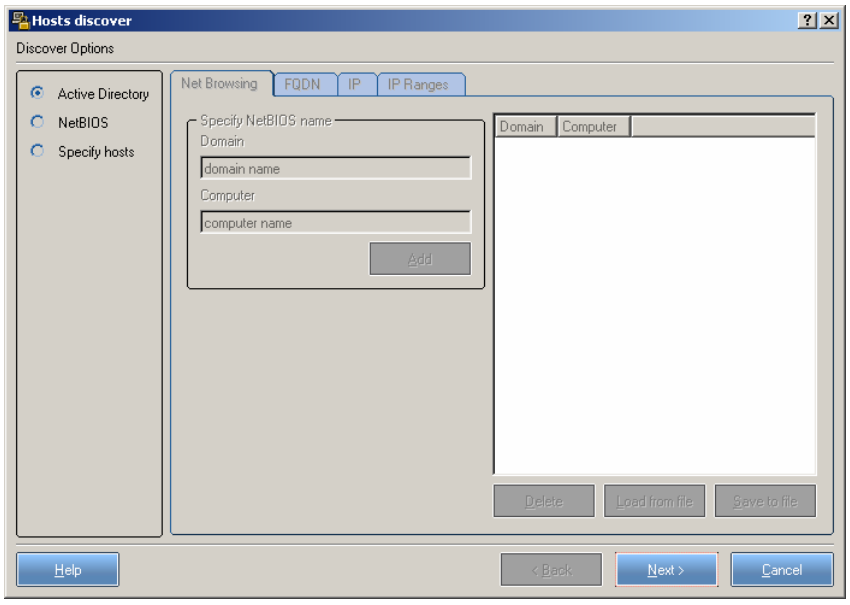
Warning: Patch Manager is a SECURITY product. It includes security-related patch information from Microsoft and Unix systems. It does NOT include usability or functional bug fix information. Due to the importance of security in today's IT environments, Patch Manager will often err in favor of providing more information in hopes of making a greater contribution to environments analyzed.

Discovering Systems

1. Run the software.
2. Click on the **Scan** button.
3. Select either the **Windows Systems** or **Unix Systems** tab.
4. Click on the **Discover...** or **Create...** button.
5. Proceed with specifying either Windows or Unix systems.

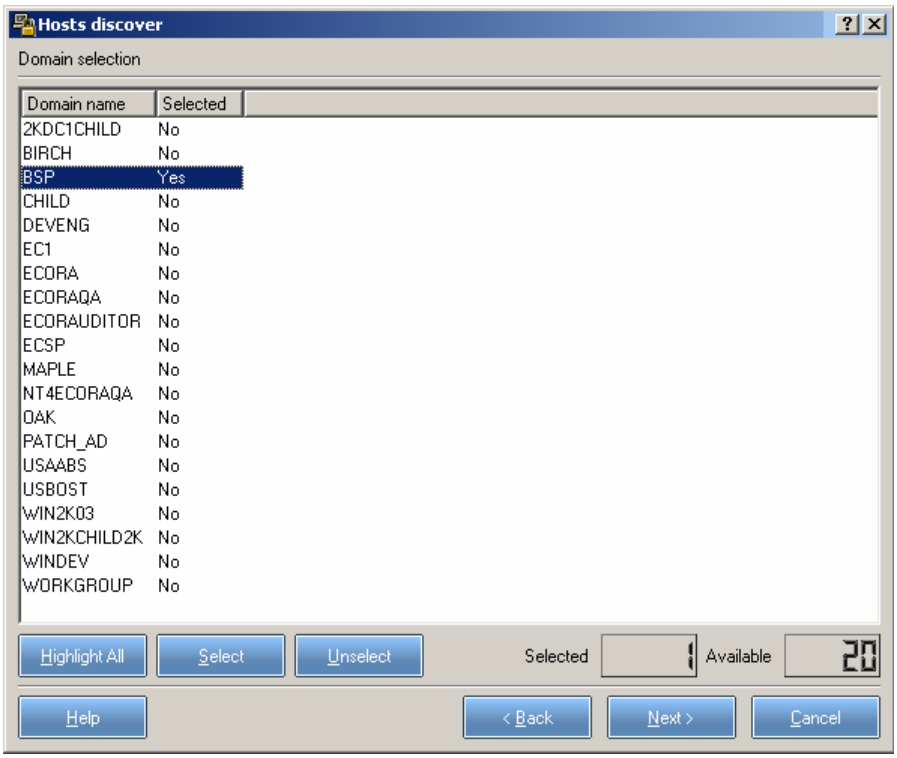
Discovering Windows Systems

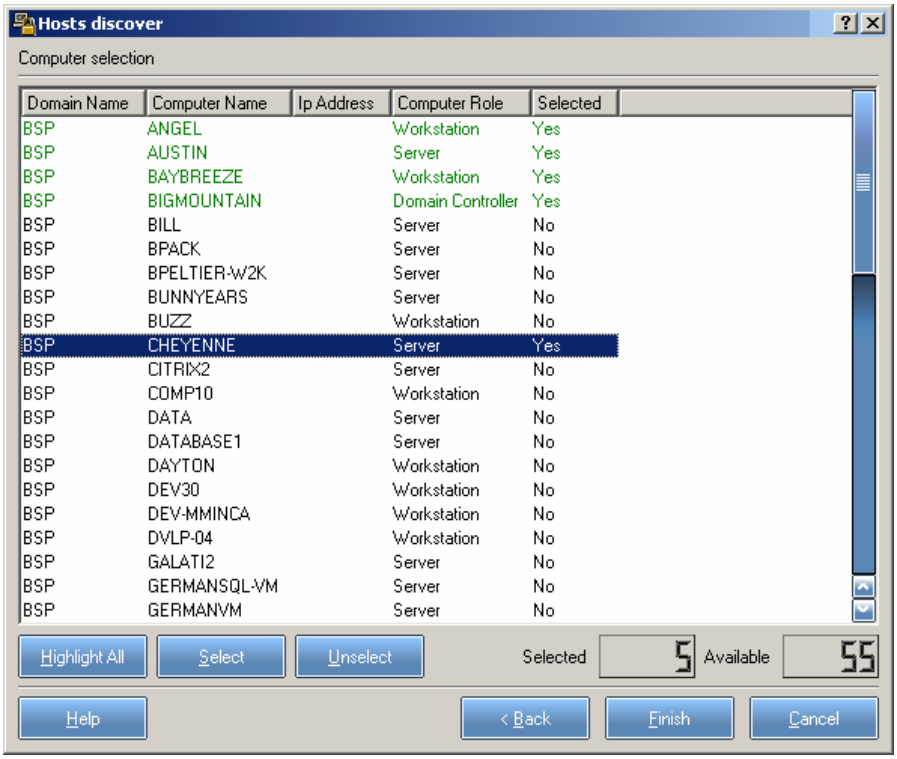
1. Select one of the following network discovery options (to find systems in the environment):
   - **Active Directory** - utilizes Active Directory tree to discover systems (proceed with step 2)
   - **NetBIOS** - utilizes NetBIOS protocol to discover systems (proceed with step 2)
   - **Specify Hosts** - allows you to manually enter, import, or specify systems in the environment (proceed to the Specifying Hosts instructions, then return to step 2).



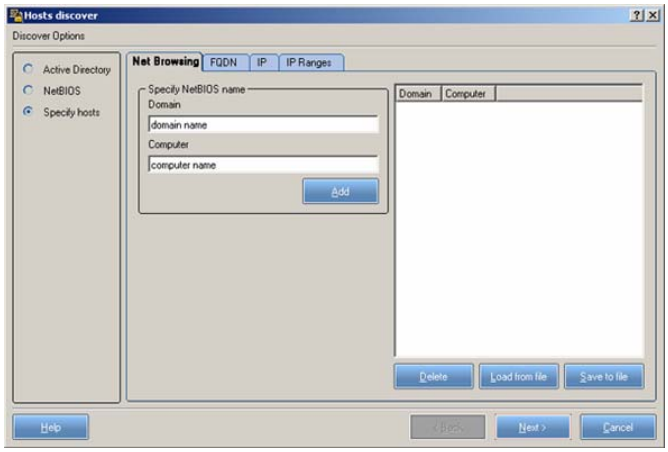
2. Click the **Next >** button.

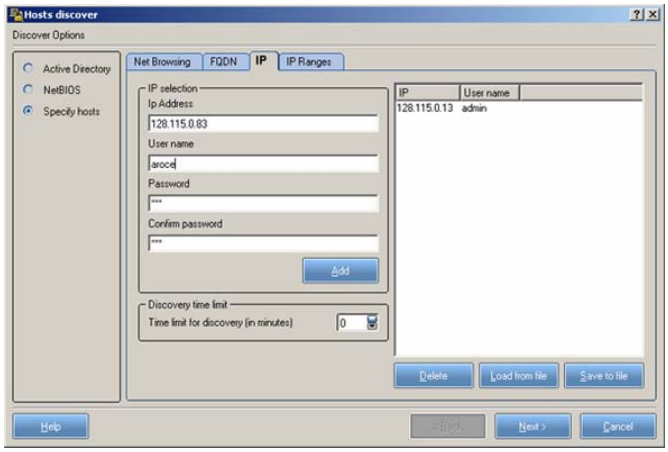
3. Select the domains in which to discover systems (double-click or use the **Select** button).
4. Click on the **Next >** button.
5. Select the discovered systems you wish to scan (double-click or use the **Select** button).
6. Click on the **Save to File** if you wish to write a text file containing these systems for re-use.
7. Click on the **Finish** button.

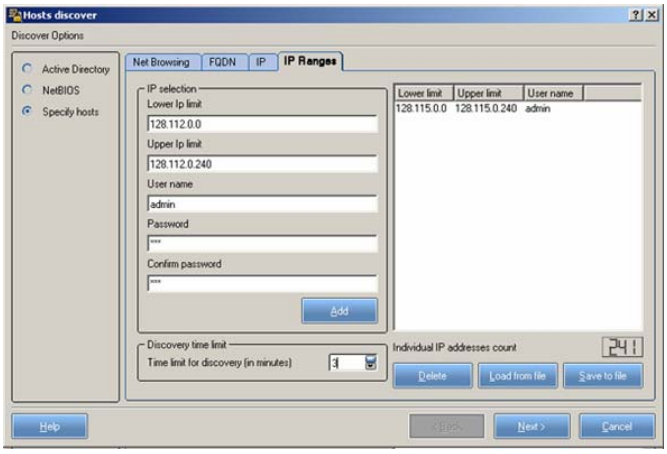




1. Since you selected **Specify Hosts**, you must select a method. Click on any or all of the following tabs:
   - **Net Browsing** - allows you to enter the domain and computer name(s) you wish to use
   - **IP** - allows you to enter the IP addresses of the systems you with to use or to import a list of IP addresses
   - **IP Ranges** - allows you to enter pair of IP addresses and discover all systems with IP addresses between them
2. On the **Net Browsing** tab, enter a domain and computer name and click **Add**.
   Note: You can also choose to save to file or load from file *(see file format)*.
3. On the **IP** tab, enter the IP address of a system.
4. Enter the username and password (and confirm the password) and click **Add**.
   Note: You can also choose to save to file or load from file *(see file format)*.
5. Enter the time limit (in minutes) during which the software will discover systems.
6. On the **IP Ranges** tab, enter a lower limit IP address and an upper limit IP address.
7. Enter the username and password (and confirm the password) and click **Add**.
   Note: You can also choose to save to file or load from file *(see file format)*.
8. Enter the time limit (in minutes) during which the software will discover systems.
9. Click on the **Next >** button.
10. Return to step 3 above.

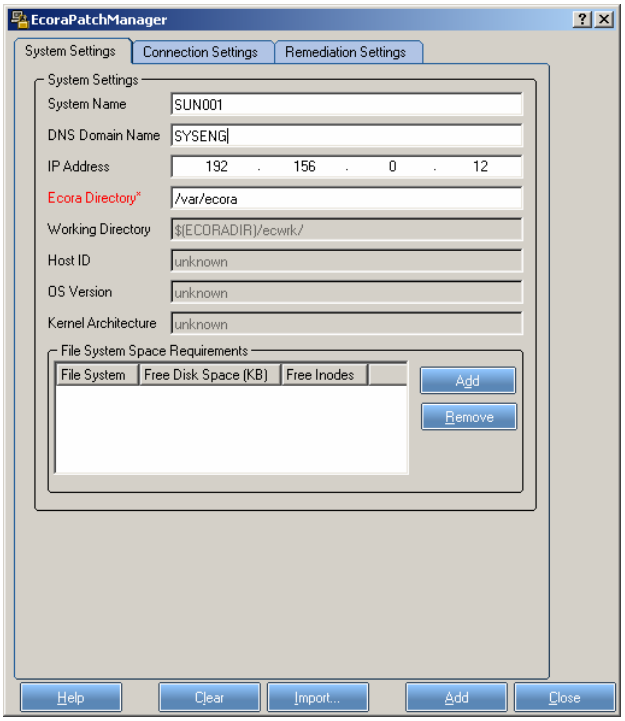


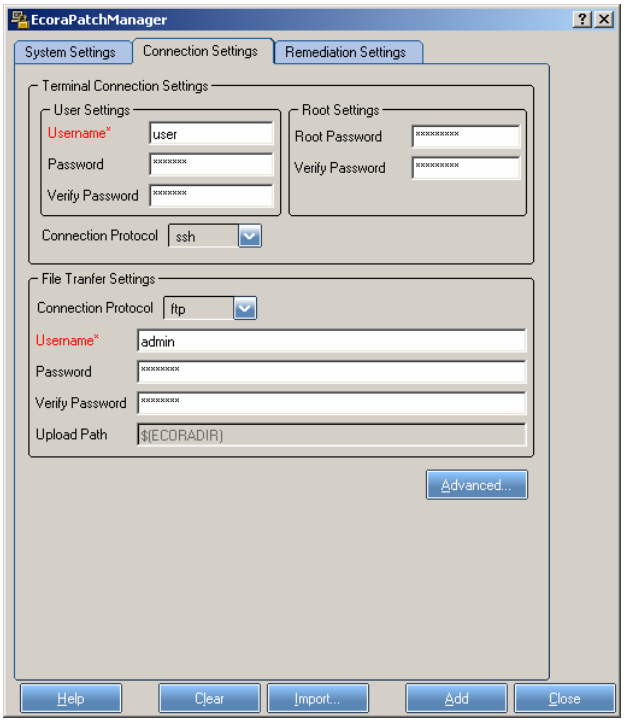




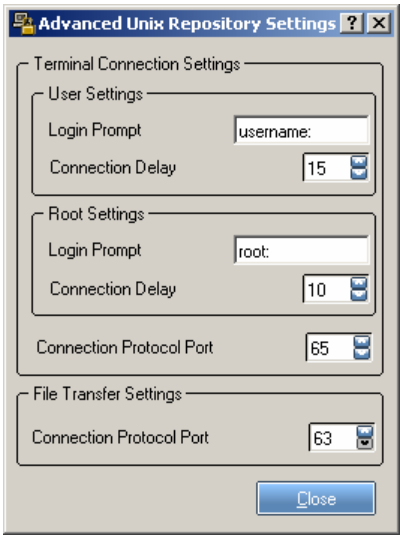
Specifying Unix Systems

1. On the **Systems Settings** tab, provide details for the system.
   Note: Fields labeled with RED text are required.
2. Enter the **System Name**.
3. Enter the **DNS Domain Name** containing the system.
4. Enter the **IP Address** of system.
5. Verify or change the **Ecora Directory** (the directory of the target machine where the Ecora software copies files).
6. Verify or change the **Working Directory**.
7. Verify the discovered Host ID, OS Version, and Kernel Architecture.
8. Use the File System Space Requirements table to define the system, disk space, and free Inodes you wish to use as minimum requirements for patch installations. If a system does not meet the requirements you set here when patch installation is attempted, the software will abort the attempt.
9. Click on the **Connection Settings** tab.
10. In the Terminal Connections Settings area, enter a Username with which to connect to the target system.
11. Enter and confirm the Password for the user name.
12. Enter the valid Root password for the system. To collect data beyond the areas the login user can access the root password for the target system is required.
13. Retype the root password to confirm that it's correct.
14. Select the Connection Protocol from the drop-down list (ssh, telnet).
15. In the File Transfer Settings area, select the Connection Protocol Port from the drop-down list (ftp, scp, sftp).
16. Enter a Username with which to transfer files.
17. Enter and confirm the Password for the user name.





18. Accept the Upload Path (not editable in this version).
19. If you wish to change ports, prompts, or delays, click the **Advanced...** button.



A. Enter or select a Connection delay milliseconds. If supplied, the software waits this length of time after logging in before attempting to transmit anything to the target system.

B. Enter the User login prompt for the repository. If supplied, the software waits for this text to appear on the connection before attempting to log into the system. If nothing is specified, it immediately attempts to login once the connection is established.

C. Enter or select a Root connection delay in milliseconds. If supplied, the software waits this length of time after logging in before attempting to transmit anything to the target system.

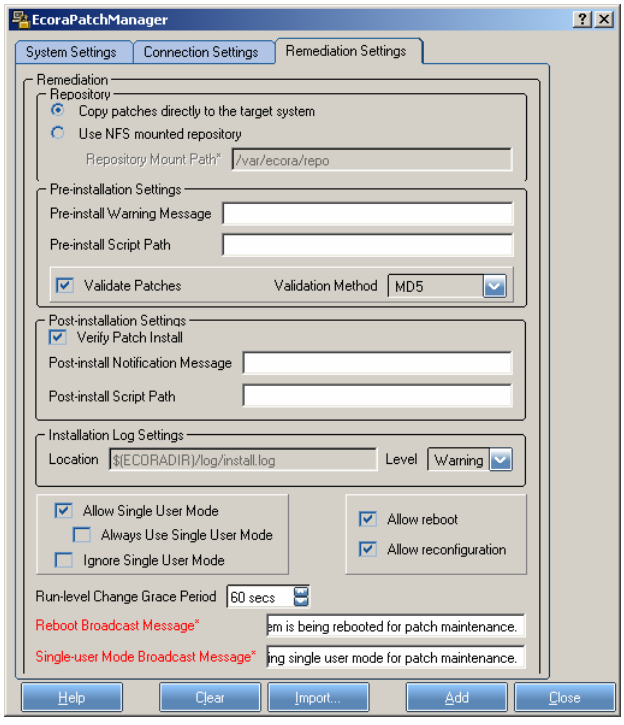
D. Enter the Root login prompt. If supplied, the software waits for this text to appear on the connection before attempting to log into the system. If nothing is specified, it immediately attempts to login once the connection is established.

E. Specify the Connection Protocol Port number for terminal connections (0 uses the default for the selected protocol).

F. Specify the Connection Protocol Port number for file transfers (0 uses the default for the selected protocol).

Tips: Entering a ZERO (0) value for any advanced settings will use the defaults. A non-zero value in any of the connection delays will cause the software to delay that amount of time after a login (or after issuing the "su" command in the case of root delay) before the software will execute any commands. The software follows the normal login procedure (send username, send password), then waits "n" milliseconds before returning "connection complete." A "non-zero" value in either of the prompt settings causes the software to, after the "normal" login procedure, search for the string entered as the users' prompt.

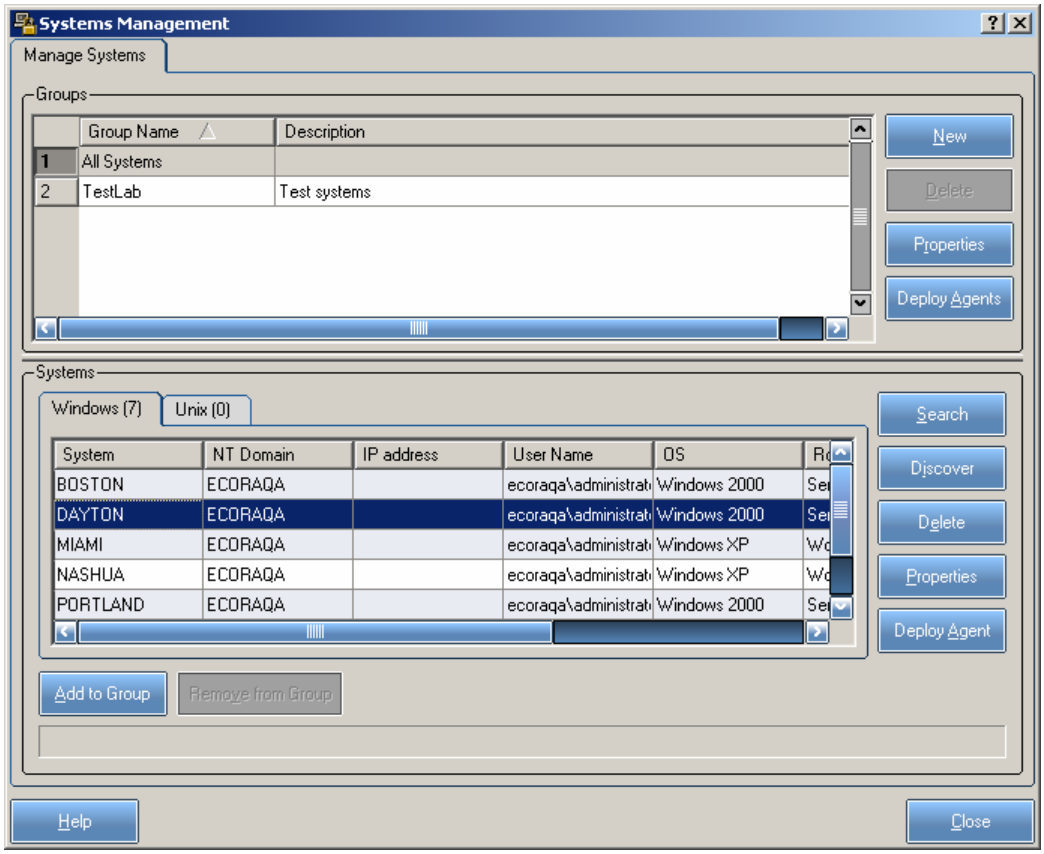
20. Click on the **Remediation Settings** tab.
21. Click in the checkbox for **Copy patches directly to the target system**.
    -OR-
    Click in the checkbox for **Use NFS mounted repository** and verify or change the Repository Mount Path.
22. Enter a pre-installation warning message (broadcast to all connected users).



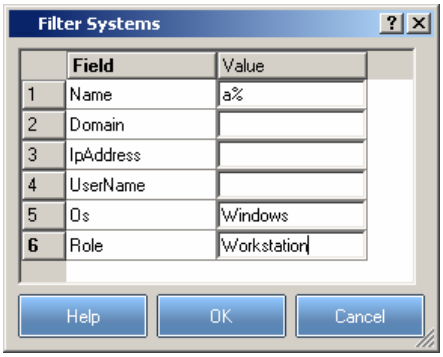
23. Enter the path to a pre-installation script if you have one that runs as standard procedure in your environment.
    Tip: Ecora suggests you create a script to run immediately before installation to stop and disable all services prior to patch installation.
24. Enable **Validate Patches** to enable checksum verification of patches at install time (before installation) and select a method (MD5 or V Sum) from the drop-down.
25. Click in the checkbox to enable **Verify Patch Install**.
    Tip: Patch installation is verified via the showrev -p command if this is enabled.
26. Enter a post-installation notification message (broadcast to all connected users).
27. Enter the path to a post-installation script if you have one that runs as standard procedure in your environment.
    Tip: Ecora suggests you create a script to run immediately after installation to re-enable and re-start all services stopped for patch installation.
28. Enter a path to the **Installation Log Settings** on target systems.
29. Select the Log level from the drop-down list.
30. Enable **Allow Single User Mode** to use single-user mode based on the vendor recommendations for each patch.
    Note: If this value is set to false, it is not possible to schedule any patches that require single-user mode; they will appear as exceptions in the analysis results.
31. Enable **Always Use Single User Mode** to handle all patches in single-user mode.
32. Enable **Ignore Single User Mode** to disregard single-user mode recommendation for patches.
33. Enable **Allow Reboot** to have Patch Manager restart systems based on the vendor recommendations for each patch.
34. Enable **Allow Reconfiguration** to change the target system settings based on the vendor recommendations for each patch.
35. Select the Run-level Change Grace Period (in seconds) from the drop-down list (the time between sending notification of a run-level change and executing the change).
36. Enter a Reboot Broadcast Message (broadcast to all connected users).
37. Enter a Single-user Mode Broadcast Message (broadcast to all connected users).
38. Use the **Clear** button to empty all fields (to specify a new system).
39. Click **Add** to save the system specifications. The software attempts to make both terminal and file transfer connections to the system to validate the information.
40. Click **Close** to implement and close.

Managing Systems & Groups

1. Run the software.
2. Choose **Tools... System Grouping...** from the menu.



3. In the Groups area, click on the **New...** button.
4. Enter a name and description for the new group and click **OK**.
5. Select the group in the Groups pane to which you wish to add system(s).
6. In the Systems pane, select those systems you wish to add to the group.
   Tip: Click **Discover** if you wish to locate additional systems.
7. Click **Add** to include the selected systems into the selected group.
8. Use the **Search...** button to locate systems by name, role, OS, etc.
9. Enter your search criteria. The search uses SQL-style queries, so % is a wildcard; entering A% in the name field will return all systems with a name starting with the letter A.



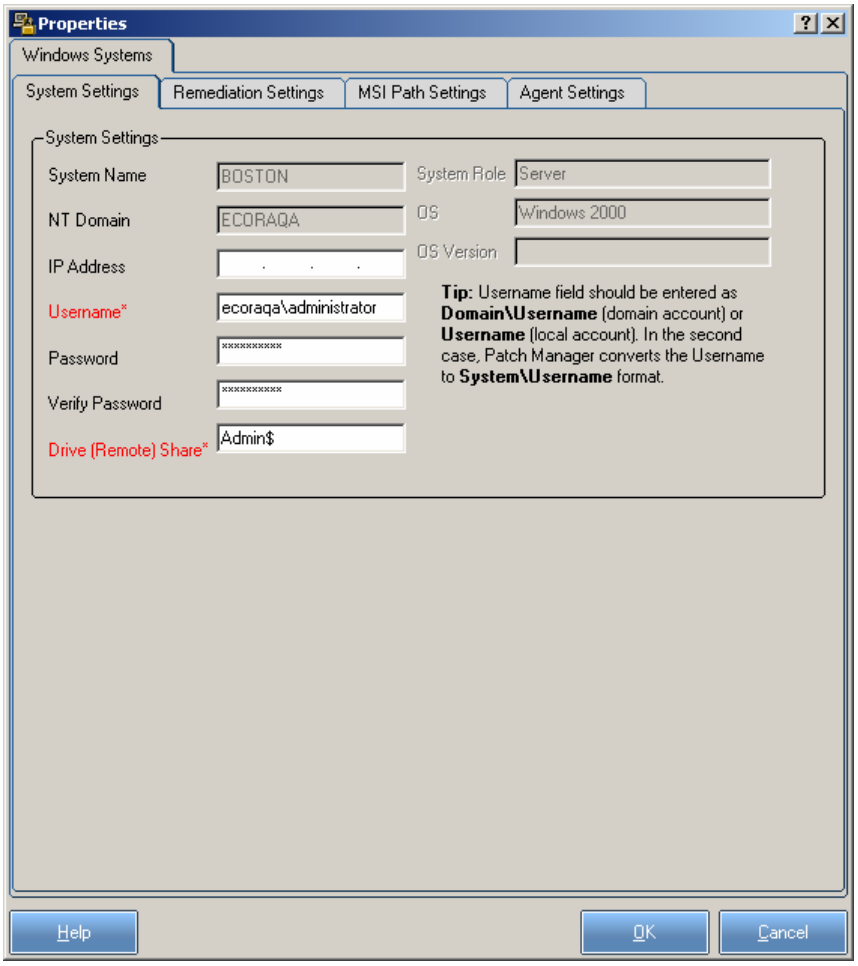
10. Select a group or system and click on the **Properties...** button.
11. Select group(s) or system(s) on which you wish to install the optional agent and click on the **Deploy Agent(s)...** button.
12. Verify or change any of the system or group attributes.
13. Click **OK**.
14. Make any additional grouping changes and click **OK**.

System & Group Properties

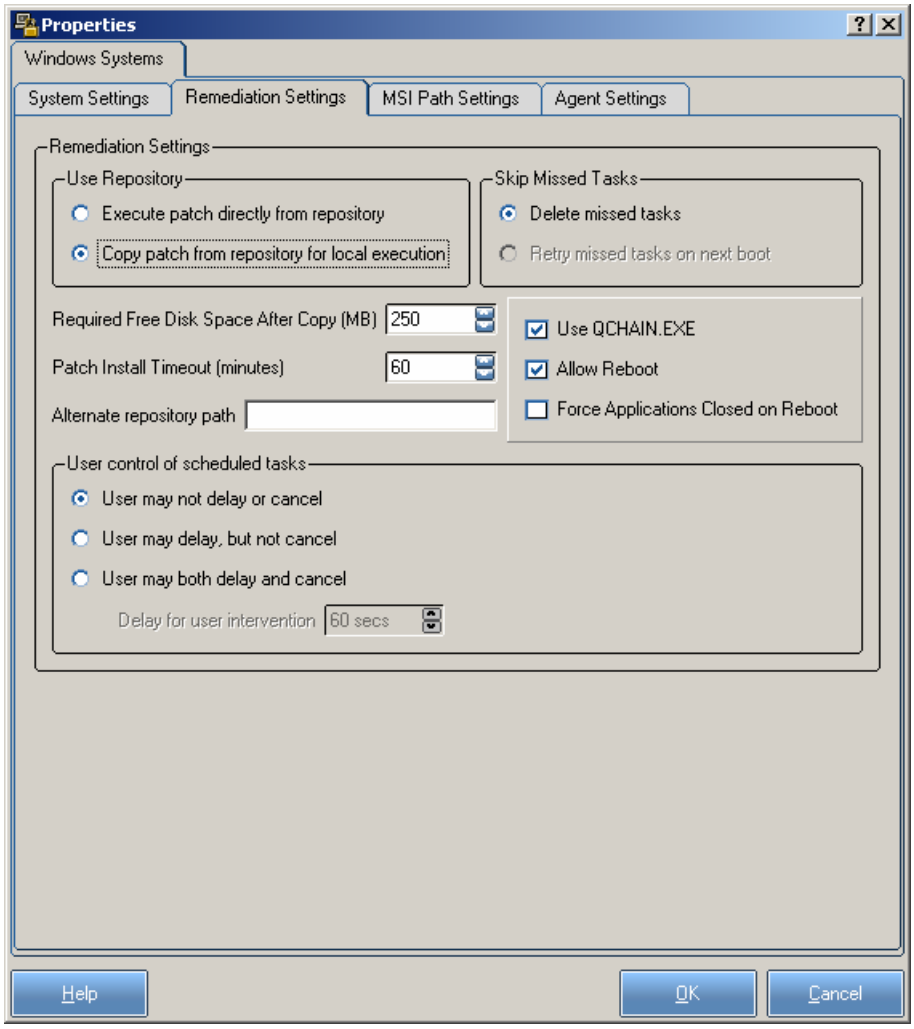
1. Run the software.
2. Click on the **Systems** button.
3. Select the **Properties...** button or right-click on an item.
4. Proceed with either Windows or Unix systems.

Windows System Properties

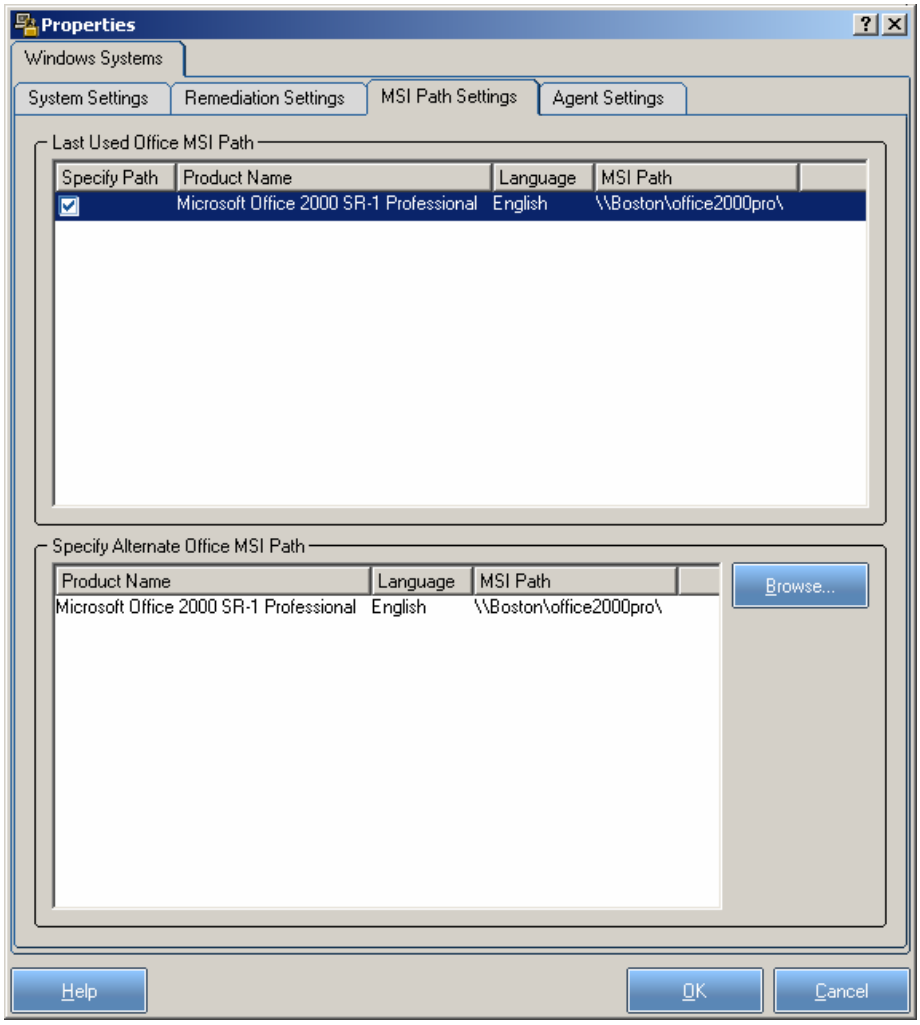
1. Click the **Properties...** button.
   Note: Fields labeled with RED text are required.
2. Click on the **System Settings** tab.
3. Enter the **System Name**.
4. Enter the **NT Domain** containing the system.
5. Enter the **IP Address** of system.
6. Confirm the **System Role**.
7. Confirm the **OS** of the system.
8. Confirm the **OS Version**.
9. Enter a Username with which to connect to the target system.
10. Enter and confirm the Password for the user name.
11. Enter the remote Drive Share.

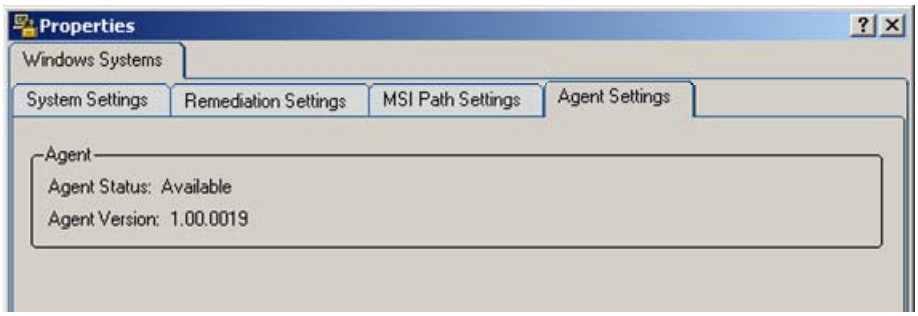


12. Click on the **Remediation Settings** tab.
13. Choose to either **Execute patch directly from repository** or **Copy patch from repository for local execution**.
14. Choose to either **Delete missed tasks** or **Retry missed tasks on next boot**.
15. Enter or select **Required Free Disk Space** (in megabytes) under which the installation will not proceed.
16. Enter or select **Patch Install Timeout** (in minutes) after which the software will abort the installation attempt.
17. If desired, enter an alternate path to the patch repository.
18. Enable any of the following options:
    Use QChain.exe (which strings patch installations together before reboot - Microsoft recommended)
    Allow Reboot (which permits the patch installer to reboot target systems if the patch vendor requires reboot)
    Force Applications Closed on Reboot (which closes all running applications, without saving, to restart the machine).
19. Enable one of the following end-user options:
    User may not delay or cancel
    User may delay, but not cancel
    User may delay and cancel
20. If you allowed user intervention, set the time, in seconds, to wait for user response.



21. Click on the **MSI Path Settings** tab.
22. Review the last-used paths to the installation CD for each MSOffice product.
23. To add an alternate path for any product, click in the **Specify Path** checkbox.
24. Use the **Browse...** button to locate an alternate path.
25. Click on the **Agent Settings** tab.
26. Review the agent version and status.
27. Click **OK**.





Understanding Scans

Once an analysis is displayed after scanning the network, the main interface is split into three window panes. The left window pane contains three tabs that allow you to choose how you wish to organize your results. The Hosts tab displays the machines analyzed. The Products tab displays the available platforms/products for which patches have been analyzed. The Patches tab displays the patches located or available for all selected systems.

The upper right window pane displays the content and properties of the patches according to the organization currently selected and active in the left pane. The lower right window pane displays the details about the currently selected item in the upper right pane, including links to in-depth articles about a selected patch.

On the Hosts tab, the left pane displays a tree control view of your network. Click on a plus to expand a level or a minus to collapse a level. At the system level, the right pane displays information relevant to that system. On the products tab, the same information is sorted by platform, OS version, or application.

The **View** buttons control the information presented:
All - Displays all available patches; installed, not detected, having a note or alert associated, that are applicable to the selected system.
Installed - Displays all patches detected as installed on the selected system.
Missing - Displays patches that are available for, but not detected on, the selected system.
Policy - Displays systems and patches (from the active scan) according to association and compliance with a defined policy.

Warning: Patch Manager is a SECURITY product. It includes security-related patch information from Microsoft, (Sun Systems, and other vendors as applicable). It does NOT include usability or functional bug fix information. Due to the importance of security in today's IT environments, Patch Manager will err in favor of providing more information in hopes of making a greater contribution to environments analyzed.

Analysis Icons

The follow icons are used in the patch analysis display:

Installed	Patch was detected as installed.
Partial Analysis / Key Installed	The Registry key indicates that the patch has been installed, but it may have been overwritten. Further research is suggested.
Missing	Patch was not detected as installed.
Warning	A DLL file that is part of this patch was detected at a higher version than expected. This is generally not problematic, but should prompt additional research and/or verification.
Note	Patch status was not conclusively determined; includes a note with more information.
Error	System could not be analyzed (no access, machine down, etc.).
Service Pack	Service pack, which is a collection of patches and hotfixes.
Patch	Patch; a piece of code that fixes, improves, or secures an existing application or operating system.
Superseded	Patch that has been superseded by a subsequent patch.
Withdrawn Patch	Patch has been withdrawn. Install the recommended patch or rollback to the approved prior revision.
Prerequisite Patch	Patch is required prior to installing a subsequent patch.
Undetermined Patch	Patch status is undetermined; evidence of the patch installation exists, but research is suggested. Check the Ecora Notes for details.
Not Required Patch	Patch is not required; this fix requires that file be changed that are not present. Not applicable.

Exception	This patch cannot be pushed due to unusual circumstances, such as the fix requiring an administrative task or a patch that requires a manual install.
Unpushable Patch	This patch cannot be pushed unless remediation settings are changed (for example, a patch that requires Single-User Mode cannot be pushed if the **Allow Single-User Mode** option has not been enabled in the System properties).
Conflict Patch	This patch cannot be pushed due to a conflict with an installed patch. This missing patch is mutually exclusive with a patch that's installed. If there are prerequisite requirements, Patch Manager attempts to determine them and provide the information in a pop-up.
Noted Patch	Patch with an associated user note.
Ecora Note Patch	Patch with an associated Ecora note.
Ignored Patch	Patch is not included in system analysis.
Approved Patch	Patch has been approved for installation or rollback by the user.
Unapproved Patch	Patch has not been approved for installation or rollback by the user.
Under Construction	This feature has not been implemented at this time.
High Risk	Patch addresses an issue rated as high risk according to CIAC (Computer Incident Advisory Committee).
Med-High Risk	Patch addresses an issue rated as medium to high risk according to CIAC (Computer Incident Advisory Committee).
Medium Risk	Patch addresses an issue rated as medium risk according to CIAC (Computer Incident Advisory Committee).
Low Risk	Patch addresses an issue rated as low risk according to CIAC (Computer Incident Advisory Committee).

Notes:

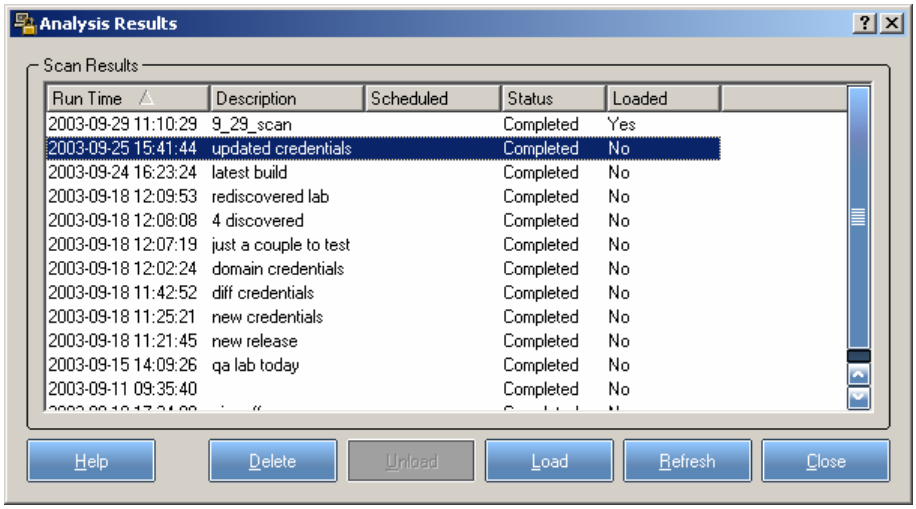
- Patch Manager tests the registry and *.dll* file versions and checksums. Other criteria associated with a hotfix can be stored in configuration metadata that cannot be readily inspected.
- If Patch Manager cannot irrevocably determine that a patch is installed, it does not mean that the patch is not installed, just that it can't be proven and Ecora would rather report conservatively than provide false assurance. Reinstalling a hotfix will probably not change the condition, as there are elements of the hotfix Patch Manager cannot evaluate.
- The Warning condition appears when a DLL associated with a hotfix is discovered to be a more recent version than was delivered in the original hotfix. This can occur when a subsequent update has replaced the original. This does not necessarily mean that the hotfix was not installed; it is just that this system did not meet all criteria. Reinstalling the hotfix will probably not change the condition, as it is Microsoft's practice not to replace newer DLLs.
- Patch Manager distinguishes unbundled and bundled (part of an OS release) Unix patches by column in the upper right pane.
- Although it does not alter the display, OS languages other than English are detected, tracked, and correct language-OS-specific patches are downloaded and applied.

Saving Scans

Once systems are scanned, the analysis results are displayed in the user interface. All results are saved to the patch knowledge database for later recall in the main interface and use by the Reporting Center. In addition, results can be exported as XML files.

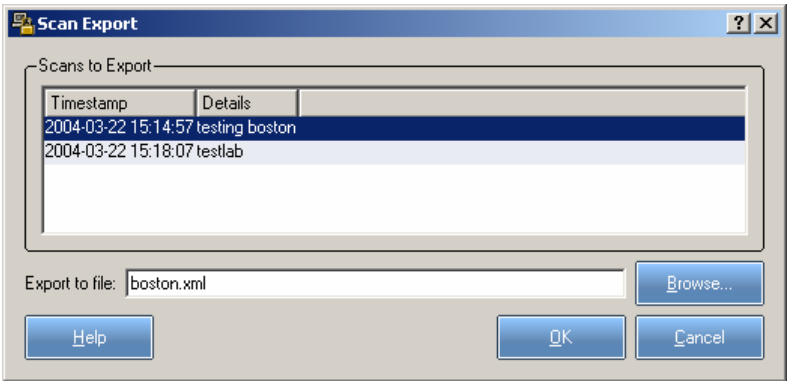
To open an existing scan:

1. Choose **File... Open Scan...** or click on the **Results** button.
2. Select the saved scan you wish to load.
3. Click **Load**.
4. Select any addition scans you wish to load.
5. Click **Load** (you can also **Delete** or **Unload** or **Refresh** scans).
6. Click **Close**.
7. Navigate the left pane tree to locate and display the scan(s) you opened.



To export the current scan as XML:

1. Scan systems you wish to analyze or open an existing scan.
2. Choose **File... Export Scans...**.
3. Select the scan to be exported.
4. Provide the name and location for saving the scan (or use **Browse** to choose a location).
5. Click **OK**.



To import existing scans:

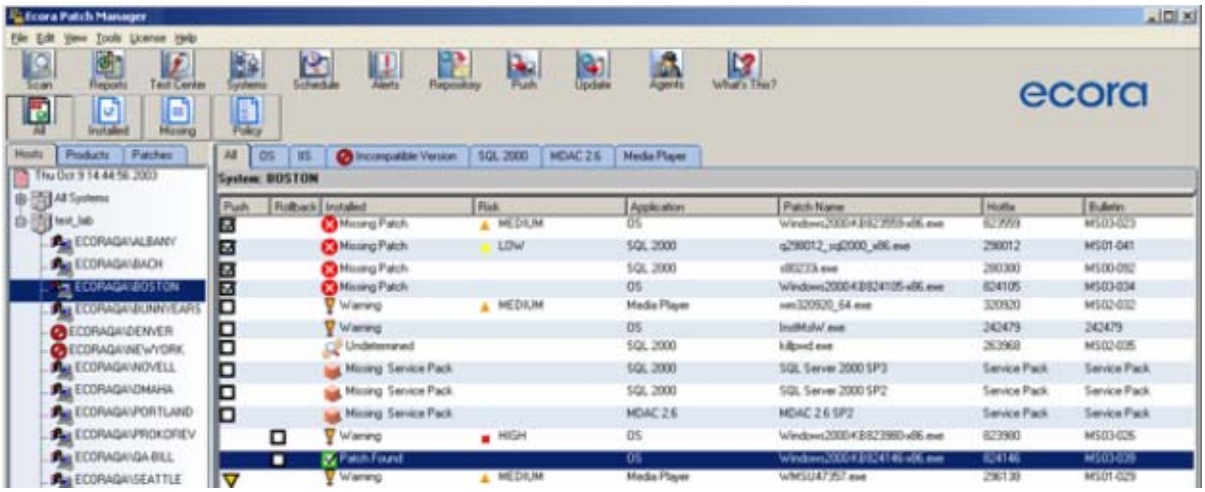
1. Choose **File... Import Scans...**.
2. Locate and select the exported scan you wish to view.
3. Click **Open**.
4. Navigate the left pane tree to locate and open the scan(s) you imported.

Installing Patches & Hotfixes

CAUTION: It is strongly recommended (for this trial and as a general practice) that all patches be tested before deployment in the production environment, particularly in environments with custom software or mission-critical applications.

See also Rollback instructions.

1. After analysis, locate the patches you wish to install.
2. In Patch or Hosts view, and optionally using the products tabs in the right pane, enable those patches you wish to install by clicking in the box in the **Push** column.



3. Once you have finished selecting patches to install, click on the **Push** button.
4. If any of the patches you selected are not already downloaded, you will be prompted to **Download** them (or Skip).
5. If prompted, manage your patch repository (collection of archived patches) and click **Download Now** or schedule download.
6. Proceed with creating (and defining settings for) a push or rollback job.

*Remediation setting defaults can be set by systems and groups (vs. individual installation jobs). Choose **Tools... Systems Grouping...**, select a system or group, click the **Properties...** button, and click on the **Remediation** tab (Windows or Unix).*

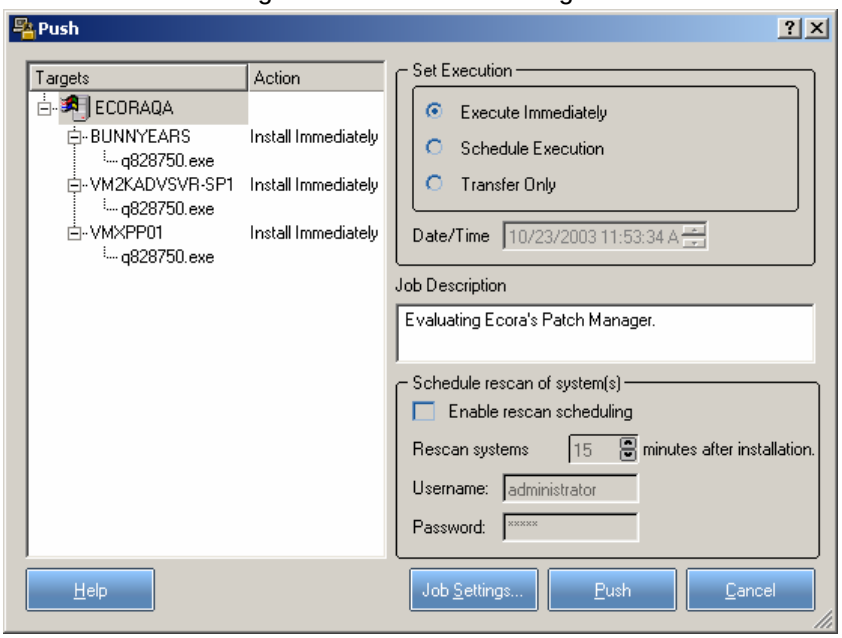
Notes: Patch Manager allows configuration of an optional user delay or cancel for installation. Some patches require user input, additional steps, or post status messages. Some MS-SQL patches require additional steps (*see instructions*).

Using Rollback

1. After analysis, locate the patches you wish to uninstall (the All or Installed views will show installed candidates for rollback).
2. In Patch or Hosts view, and optionally using the products tabs in the right pane, enable those patches you wish to uninstall by clicking in the box in the **Rollback** column.
3. Once you have finished selecting patches to rollback, click on the **Push** button.
4. Proceed with creating a push or rollback job.

Push & Rollback Jobs

1. In the Push dialog box, click on the plus sign to expand the tree and verify that the systems and patches are correct.
2. Select an option to enable:
   Execute Immediately if you would like install/uninstall now
   Schedule Execution to set a later time and date for deployment.
   Transfer Only to copy files to the target without installing
3. If you enabled scheduling, set the date and time using the up/down arrows.
4. Enter a job description to be used in scheduling and written to the log file.
5. Click in the checkbox to **Enable rescan scheduling** if you wish to have Patch Manager scan after execution to verify that patches were installed / rolled back as intended.
6. If you enabled rescan, set the time, in minutes, after job execution to have Patch Manager scan and enter a username and password.



   Tip: Re-scan results must be opened by choosing **File... Open Scan...** after the elapsed time.

7. Click **Job Settings...** to set job settings.
8. Click **Push** to begin installation (per the above settings) of the selected patches.
9. After successful deployment, you can **Scan** or choose **View... View Patch Log** to verify that the patch deployment succeeded.

   Note: Some patches require user input, additional steps, or post status messages. Some MS-SQL patches require additional steps (*see instructions*).

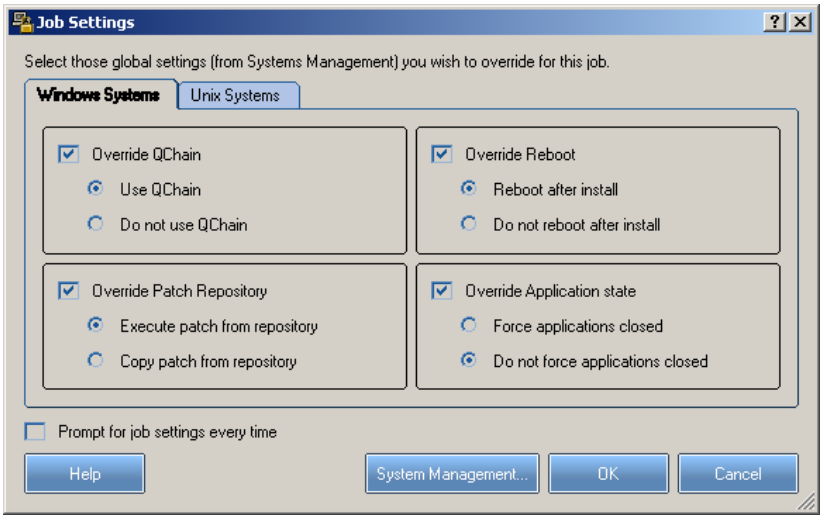
Job Settings

You have the ability to customize your settings, including overriding (for this job only) the global settings you have established in system properties.

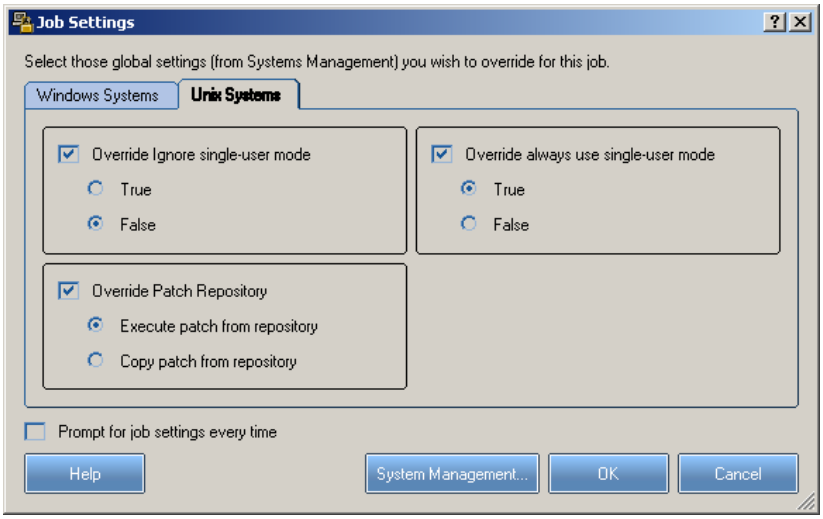
To change the settings:

1. Click the **Job Settings...** button.
2. Click on the **Windows Systems** tab.

3. Click the **Override QChain** option if you wish this job to deviate from your global settings. QChain strings patch installations together before reboot - Microsoft recommended.
4. If you enabled Override QChain, select **Use QChain** or **Do not use QChain**.
5. Click the **Override Patch Repository** option if you wish this job to deviate from your global settings.
6. If you enabled Override Patch Repository, select **Execute patch from repository** or **Copy patch from repository**.
7. Click the **Override Reboot** option if you wish this job to deviate from your global settings. Reboot permits the patch installer to reboot the machine if Microsoft requires reboot.



8. If you enabled Override Reboot, select **Reboot after install** or **Do not reboot after install**.
9. Click the **Override Application State** option if you wish this job to deviate from your global settings.
10. If you enabled Override Application State, select **Force applications closed** or **Do not force applications closed**. **Force Applications Closed on Reboot** exits all running applications, without saving, to restart the machine.
11. Click on the **Unix Systems** tab.
12. Click the **Override Ignore Single-User Mode** option if you wish this job to deviate from your global settings.
13. If you enabled Override Ignore Single-User Mode, select **True** or **False**.
14. Click the **Override Always Use Single-User Mode** option if you wish this job to deviate from your global settings.



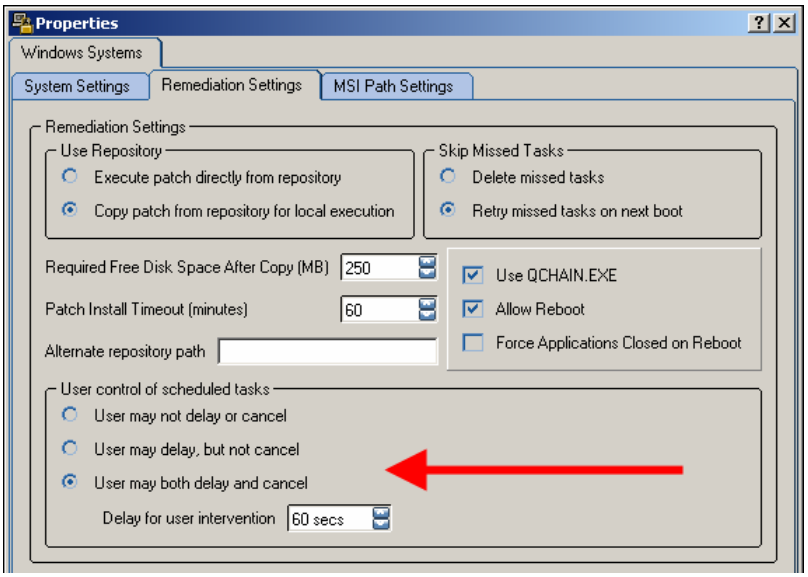
15. If you enabled Override Always Use Single-User Mode, select **True** or **False**.
16. Click the **Override Patch Repository** option if you wish this job to deviate from your global settings.

17. If you enabled Override Patch Repository, select **Execute patch from repository** or **Copy patch from repository**.
18. Enable the checkbox to **Prompt for job settings every time** if you wish to have a chance to change these settings each time.
19. Click on the **Systems Management...** button if you wish to change any global settings.
20. Click **OK**.

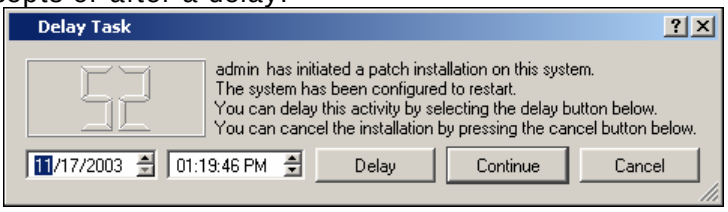
User Delay

To accommodate users working at systems you are attempting to patch and/or reboot, Patch Manager includes an optional user delay. This feature is a dialog box in which the user can cancel or delay the patch installation you have sent to their system.

To allow user control / delay:



1. Choose **Tools... Systems Grouping...**.
2. Select a system or group and click on the **Properties...** button.
3. Click on the **Remediation** tab.
4. Enable one of the user control options:
   User may not delay or cancel - installation proceeds without allowing any user intervention.
   User may delay, but not cancel - installation proceeds once the delay time elapses.
   User may delay and cancel - installation proceeds only if the user accepts or after a delay.
5. If you allow users to delay, set the time, in seconds, in which the user must respond to the prompt.
6. Click **OK**.


Delay Task
admin has initiated a patch installation on this system.
The system has been configured to restart.
You can delay this activity by selecting the delay button below.
You can cancel the installation by pressing the cancel button below.
11/17/2003
01:19:46 PM
Delay
Continue
Cancel

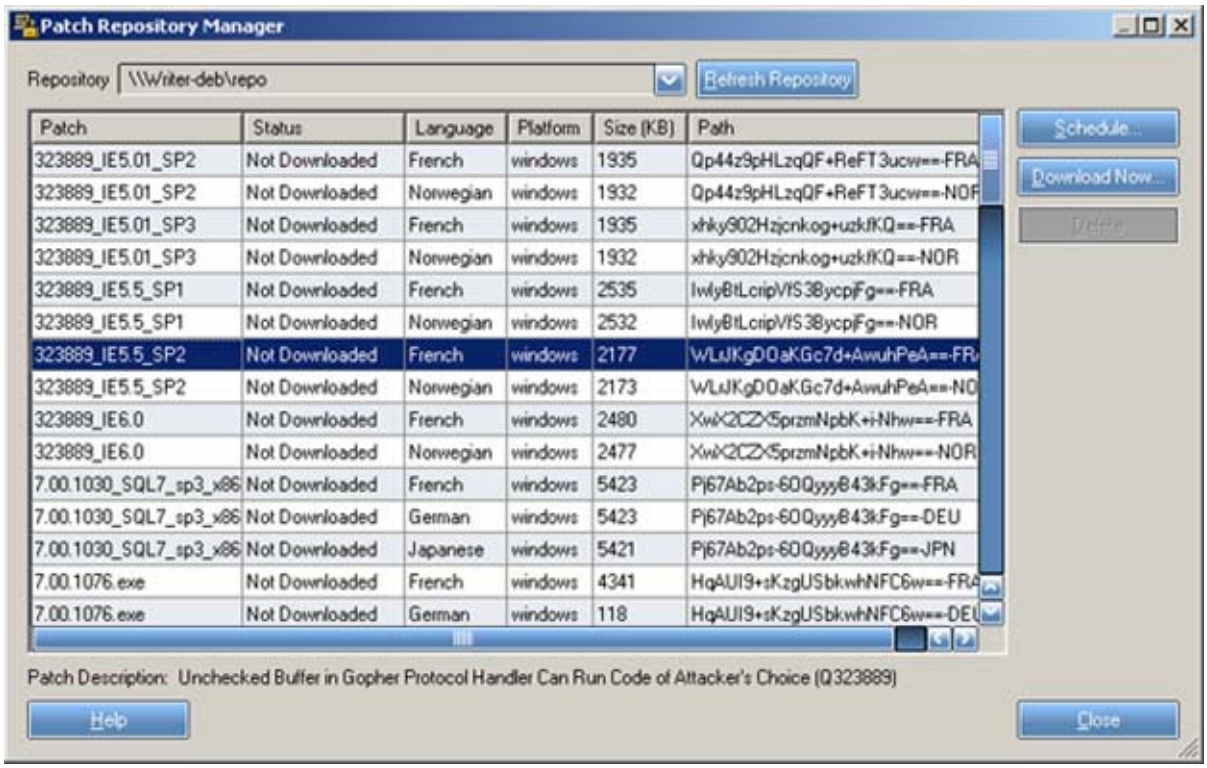
If user control is enabled, end users at target systems being patched are prompted to delay (or cancel) the patch installation. If the user elects to delay, they set the date and time to run the task again (in the drop-downs to the left) and they are prompted again at that time. If they elect to cancel (if that option is enable), the task and associated files are deleted and the patch are not installed. If there is no user response, the installation proceeds after the delay established in the properties.

Note: This section describes the delay on Windows systems. Unix users can receive a pre-installation warning message if configured in the Unix system properties.

Patch Repository Management

A repository is the location where patches will be downloaded and maintained. You MUST specify a Windows Repository to install the online Reporting Center and any Windows patches. If you intend to support any Unix systems with Patch Manager, you must specify a Unix Repository as well. In both cases, select locations with sufficient disk space to accommodate storing patches and service packs.

1. Choose **Tools... Repository Management...** to access the Repository Manager.


Patch Repository Manager
Repository
\\Writer-deb\repo
Refresh Repository
Patch
Status
Language
Platform
Size (KB)
Path
323889_IE5.01_SP2 Not Downloaded French windows 1935 Qp44z9pHLzqQF+ReFT3ucw==-FRA
323889_IE5.01_SP2 Not Downloaded Norwegian windows 1932 Qp44z9pHLzqQF+ReFT3ucw==-NOR
323889_IE5.01_SP3 Not Downloaded French windows 1935 xhky902Hzjcnkog+uzkfKQ==-FRA
323889_IE5.01_SP3 Not Downloaded Norwegian windows 1932 xhky902Hzjcnkog+uzkfKQ==-NOR
323889_IE5.5_SP1 Not Downloaded French windows 2535 IwlyBtLcripVfS3BycpjFg==-FRA
323889_IE5.5_SP1 Not Downloaded Norwegian windows 2532 IwlyBtLcripVfS3BycpjFg==-NOR
323889_IE5.5_SP2 Not Downloaded French windows 2177 WLuJKgDOaKGc7d+AwuhPeA==-FR
323889_IE5.5_SP2 Not Downloaded Norwegian windows 2173 WLuJKgDOaKGc7d+AwuhPeA==-NO
323889_IE6.0 Not Downloaded French windows 2480 XwX2CZX5przmNpbK+i+Nhw==-FRA
323889_IE6.0 Not Downloaded Norwegian windows 2477 XwX2CZX5przmNpbK+i+Nhw==-NOR
7.00.1030_SQL7_sp3_x86 Not Downloaded French windows 5423 Pj67Ab2ps-6OQyyyB43kFg==-FRA
7.00.1030_SQL7_sp3_x86 Not Downloaded German windows 5423 Pj67Ab2ps-6OQyyyB43kFg==-DEU
7.00.1030_SQL7_sp3_x86 Not Downloaded Japanese windows 5421 Pj67Ab2ps-6OQyyyB43kFg==-JPN
7.00.1076.exe Not Downloaded French windows 4341 HqAUI9+sKzgUSbkwhNFC6w==-FRA
7.00.1076.exe Not Downloaded German windows 118 HqAUI9+sKzgUSbkwhNFC6w==-DEU
Schedule...
Download Now...
Delete
Patch Description: Unchecked Buffer in Gopher Protocol Handler Can Run Code of Attacker's Choice (Q323889)
Help
Close

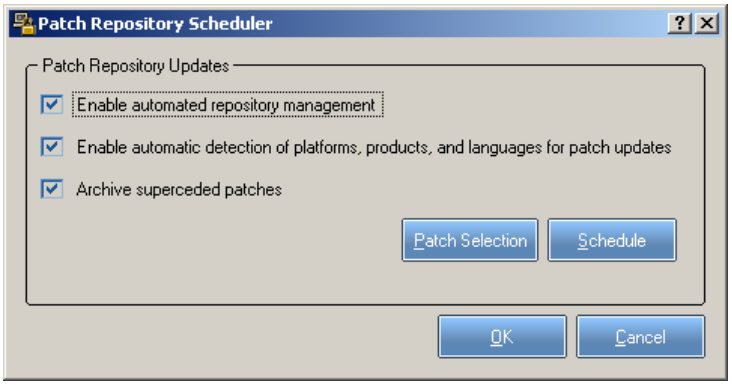
2. Select a repository to review from the drop-down list.
3. Click the **Refresh Repository** button to load the most current information available into the display.
4. Review the patches in the active repository, using the column headings to sort on various information.
5. Click on the **Schedule...** button to set up automated checks for new patches and repository maintenance.
6. Click on the **Download Now...** button to download a more current version of the selected patch.
7. Click on the **Delete** button to remove the selected patch from the active repository.
8. Click the **Close** button to accept changes and close the dialog box.

Tip: The Windows and Unix repositories are established via **File... Settings... Repository** tab.

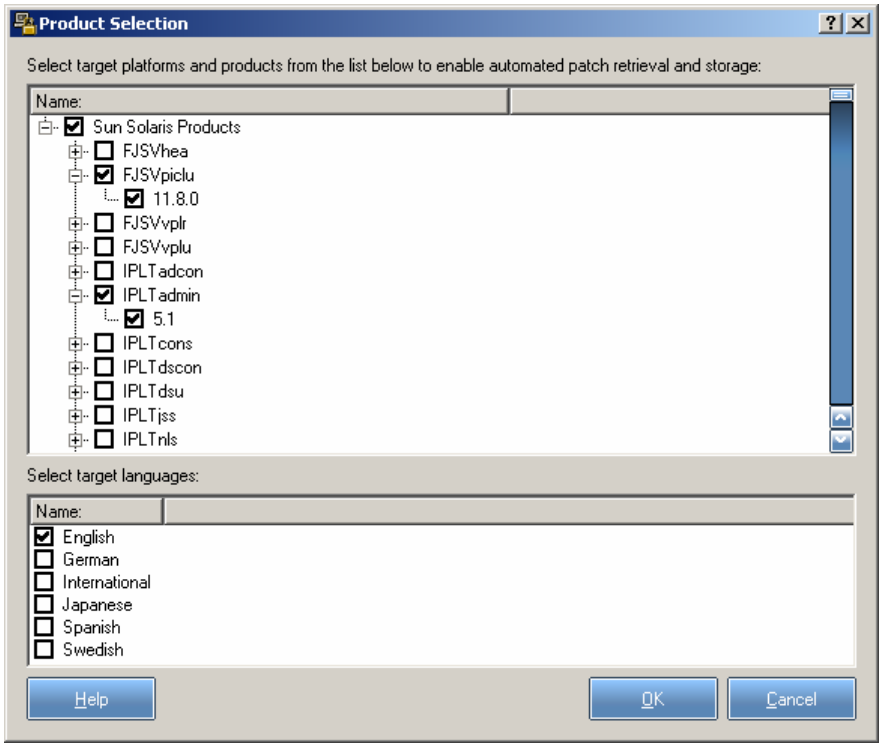
Patch Repository Maintenance

Establishing automatic repository maintenance allows you to select patches (by past scans or by product) that you want to ensure are always current and downloaded in the repository. You select which patches will be maintained and on what schedule, and Patch Manager's background service does all the detection, downloading, and administration (such as changing the status in the repository) without any intervention or prompting.

1. In the Patch Repository Scheduler dialog box, enable **Automated repository management** if you want to maintain current patches by product. You must select the products and platforms you wish to maintain.
2. Enable **Enable automatic detection of platforms, products, and languages for patch updates** if you want Patch Manager to maintain current copies of missing patches from existing scans.
   Tip: If you enable the first two options, but enable nothing under patch selection, Patch Manager will download current copies of any patch detected as missing in any of your existing scans. This is basically a shortcut to selecting which products to maintain; this option downloads all "relevant" patches based on scans.
3. Enable **Archive superseded patches** if you wish to maintain archived copies of patches replaced by newer versions. These archived copies are renamed and maintained in the repository, not moved or deleted.



4. Click on the **Patch Selection...** button to choose which operating systems and/or applications will be handled by automated repository maintenance.
5. Click on the plus signs to expand the tree.
6. Click in any checkbox to select that application / OS and its patches.
   Tip: To select only some child objects, expand the tree, but do not select the top-level object. Instead, select the child / subordinate objects.



7. In the lower pane, select the language(s) you wish to support and maintain.
8. Click on the **Schedule...** button to set up the dates, times, schedule, and automated recurrence of repository maintenance.
9. Click **OK**.
10. Click the **Close** button to accept changes and close the dialog box.

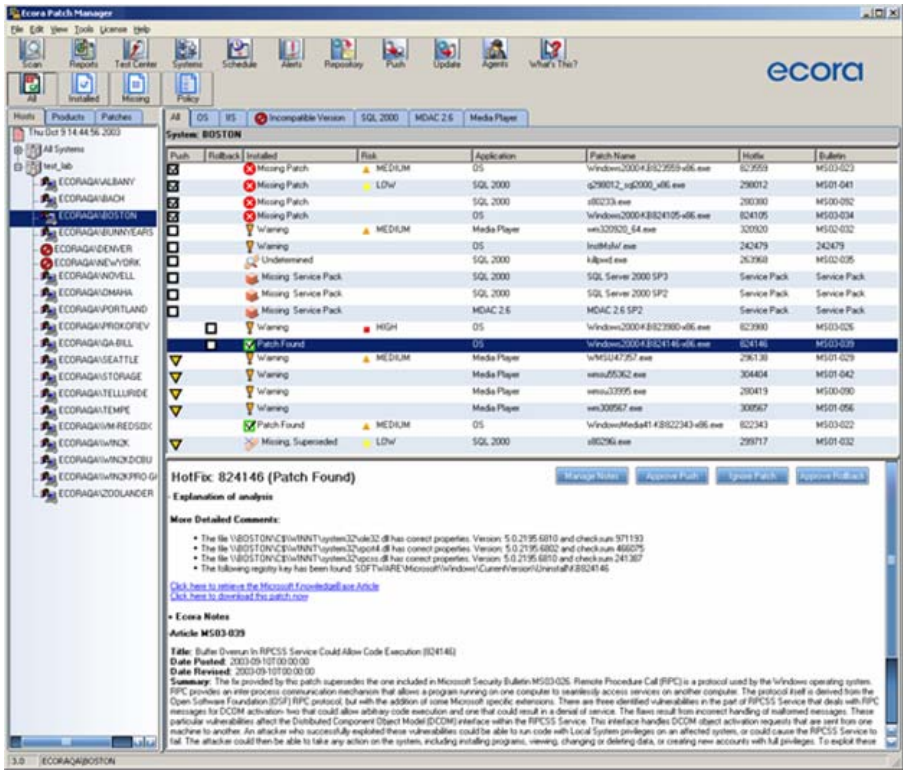
Tip: If you need to operate without Internet connectivity, update manually or create an installation with repository on a machine with Internet connectivity, maintain updates and current patch downloads there, and periodically cut CDs to update the secure machine hosting the real installation and repository.

Tip: If you need to change or correct the credentials provided for the Ecora Patch Service used for repository maintenance:
In Patch Manager, go to **File... Settings...** and update them on the **Preferences** tab.
OR
In Windows, go to the Control Panel, locate Service Control Manager (under Admin Tools in some versions), locate the Ecora Patch Service, click RIGHT, choose **Properties**, and update the on the **Log On** tab.
After either, verify that the service is RUNNING.

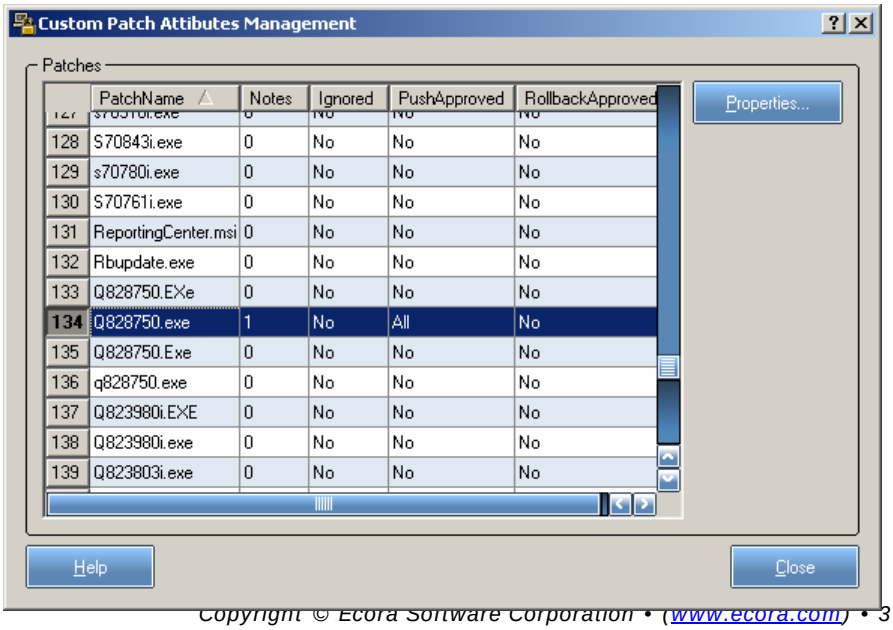
Patch Notes & Properties

Patch Manager provides the ability to add notes and conditions to each patch. This allows you to record your test findings or comments, approve patches for push (installation) or rollback, and set certain patches to be ignored in analysis.

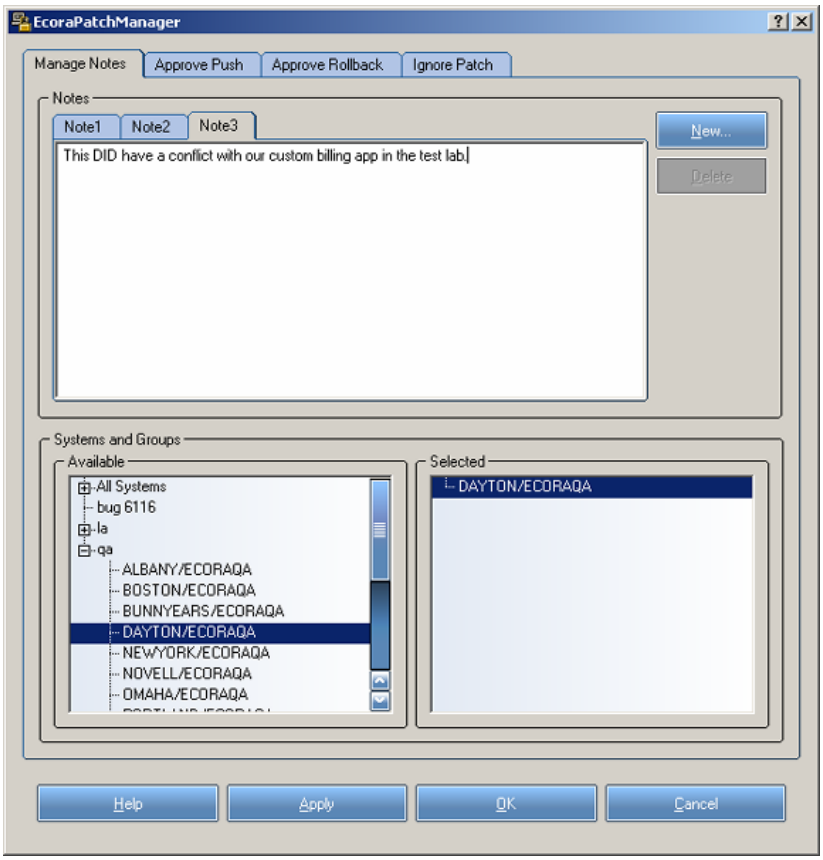
Once a scan is completed and the right pane populated, select a patch to see the details. For any given patch, you may click one of the buttons to alter the patch properties or access **Tools... Custom Notes Management...** from the main menu.

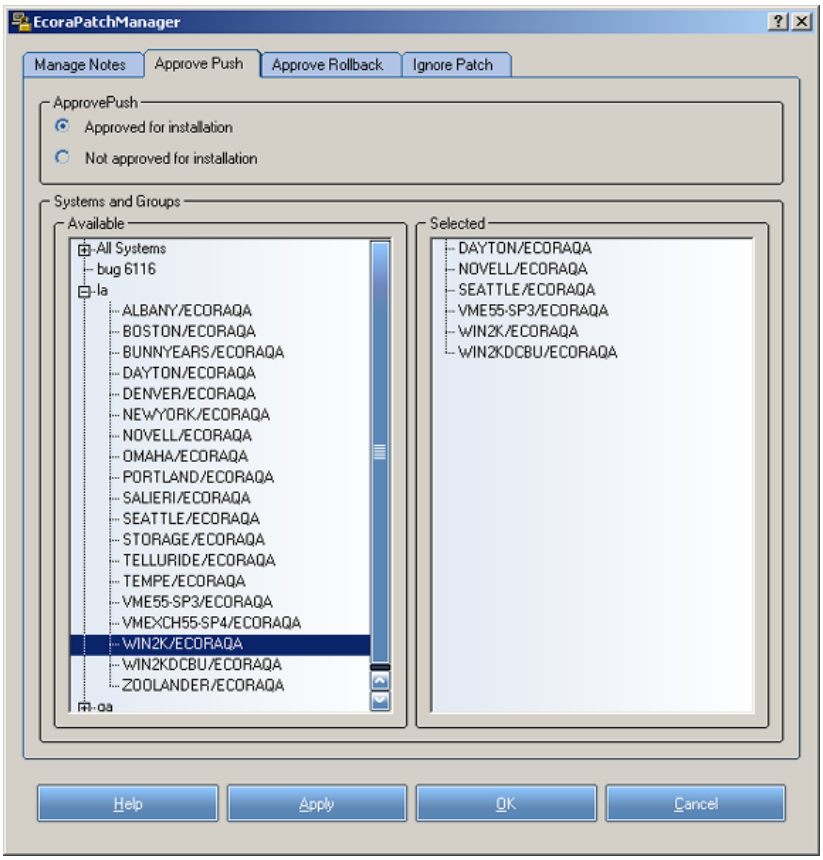


1. Choose **Tools... Custom Notes Management...** from the main menu.
2. Select the patch for which you wish to modify or add notes or properties.
3. Click the **Properties...** button.

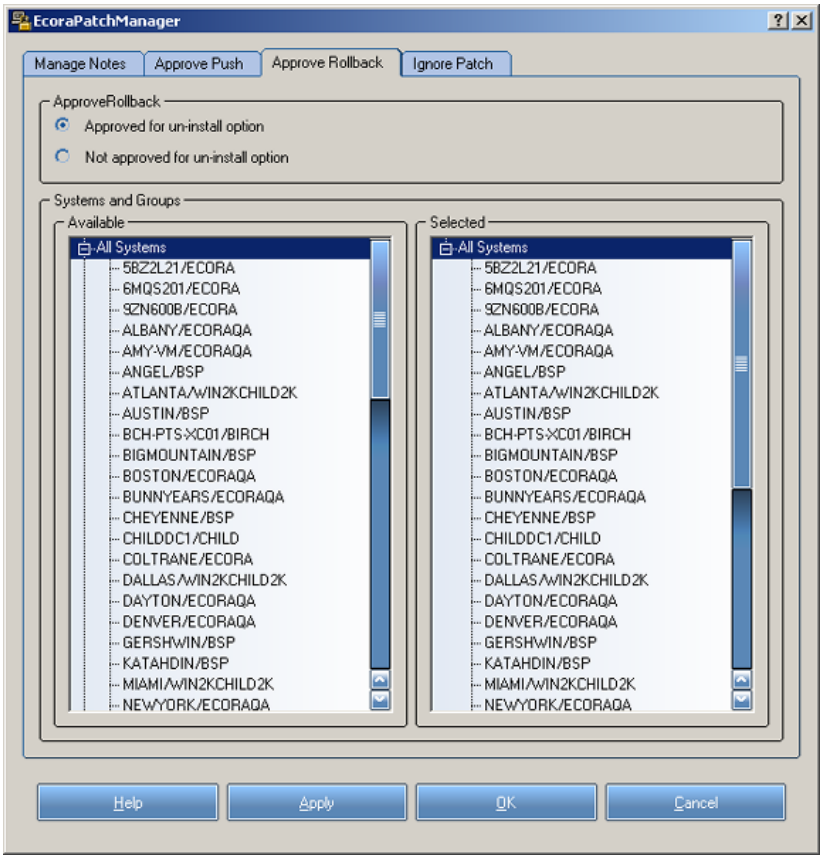


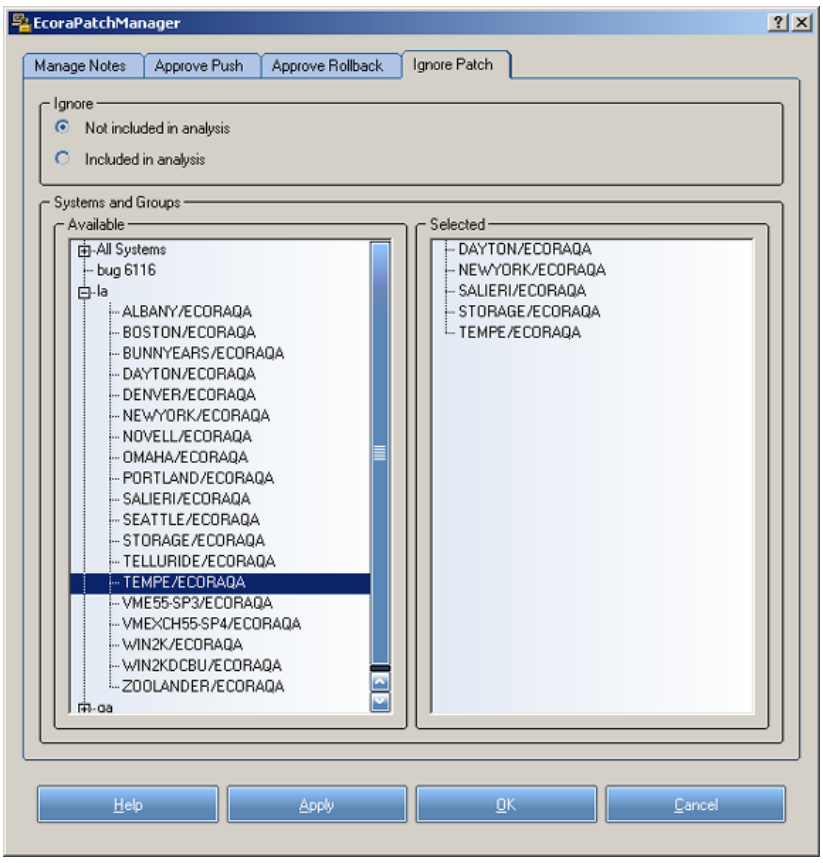
4. On the **Manage Notes** tab, select an existing note tab or click the **New...** button.
5. Name the Note (or accept the numbered default) and click **OK**.
6. Place the cursor in the text field and enter or edit text for the note.
7. Double-click on a node in the lower left pane, use the expandable tree to locate and select groups or system to which this note applies. Verify the selected systems in the lower-right results pane.
8. Click the **Apply** button.
9. Click on the **Approve Push** tab.
   Tip: To enable approvals, choose **File... Settings...** and click in the **Require approval for installation / rollback** checkbox.
10. Click in the radio button for **Approved for installation** or **Not approved for installation** for this patch.
11. Double-click on a node in the lower left pane, use the expandable tree to locate and select groups or system to which this note applies. Verify the selected systems in the lower-right results pane.
12. Click the **Apply** button.





13. Click on the **Approve Rollback** tab.
    Tip: To enable approvals, choose **File... Settings...** and click in the **Require approval for installation / rollback** checkbox.
14. Click in the radio button for **Approved for un-install option** or **Not approved for un-install option** for this patch.
15. Double-click on a node in the lower left pane, use the expandable tree to locate and select groups or system to which this note applies. Verify the selected systems in the lower-right results pane.
16. Click the **Apply** button.
17. Click on the **Ignore Patch** tab.
18. Click in the radio button for **Not included in analysis** or **Included in analysis** for this patch.
    Tip: To see which patches are being ignored, click on the **All** button in the **View** toolbar.
19. In the lower left pane, use the expandable tree to locate and select groups or system to which this note applies. Verify the selected systems in the lower-right results pane.
20. Click the **Apply** button.
21. Click the **OK** button to close.





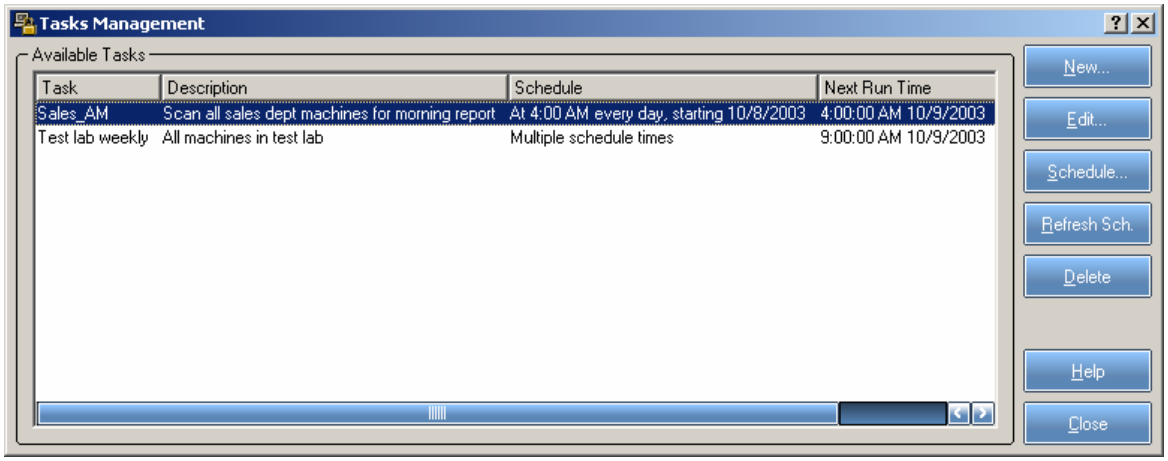
Scheduling Patch Analysis

The scheduling function allows you to set Patch Manager to run automatically any time you choose. Scan systems after work so data is ready at the start of the day... or at the end of each quarter to prepare for regular audits. Within an international 24 x 7 enterprise, schedules can be set to run at different times for multiple locations, so that data is available for local, multi-site use at appropriate times. Incorporate scheduling to automate maintenance and disaster readiness procedures.

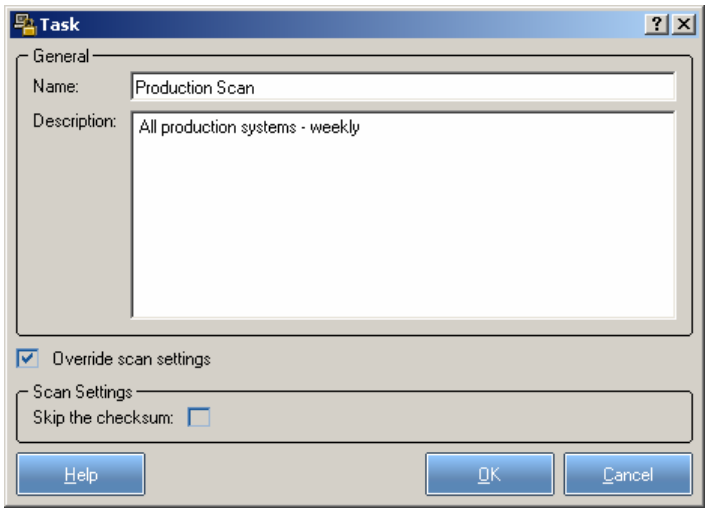
Scheduling Scans
Windows Task Scheduler
Scheduling Updates

Scheduling Scans

1. Click on the **Schedule** button (or choose **Tools... Schedule Scans...**).



2. Click on the **New...** button (or select an existing task to **Edit** or **Delete**).
3. Enter a name and description for the new task.
4. Enable **Override Scan Settings** if you do NOT wish to use your usual choices.
5. If you chose to **Override Scan Settings**, enable or disable **Skip Checksum** analysis.
6. Click **OK**.
7. In the Systems Selection dialog, select the systems you wish to scan in this task.
8. Proceed in Windows Task Scheduler.



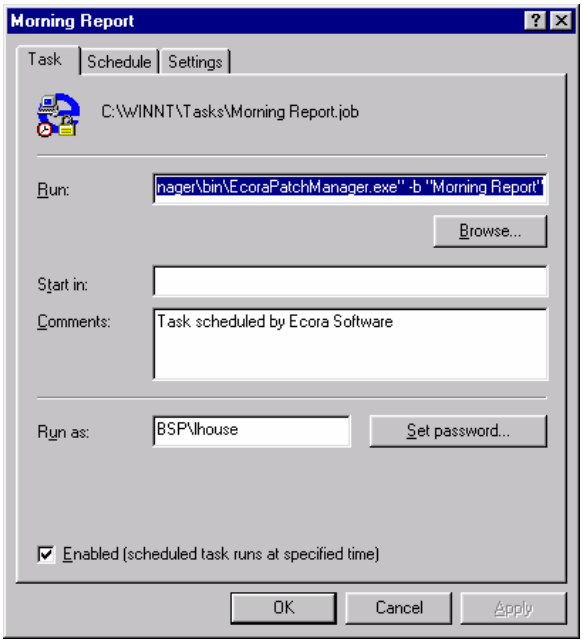
Tip: To schedule recurring agent scans, see Scheduling Agent Analysis.

Windows Task Scheduler

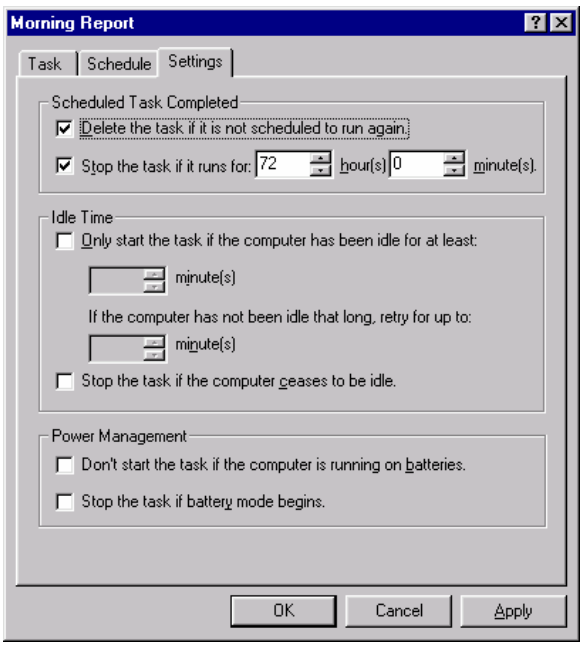
1. In Windows Task Scheduler, on the Task tab, verify the program to be run.
2. Verify the program directory and comments.
3. Choose the user for the **Run as** field and use the **Set Password...** button to enter a password if one is required for administrative access.
4. Verify that the **Enabled** checkbox is active for the task with run as scheduled.
5. Click on the **Schedule** tab.
6. Click **New** to create a schedule or select an existing one from the drop-down list.

10. On the Settings tab, set any time limits for the task, Idle Time required, or Power Management preferences.
11. Click **Apply**.
12. Click **OK**.

For information on upgrading scheduled tasks, see Troubleshooting.



7. Set the day, time, and frequency for the task.
8. Click in the **Show Multiple Schedules** checkbox if you wish to view more than one task.
9. Click on the **Settings** tab.

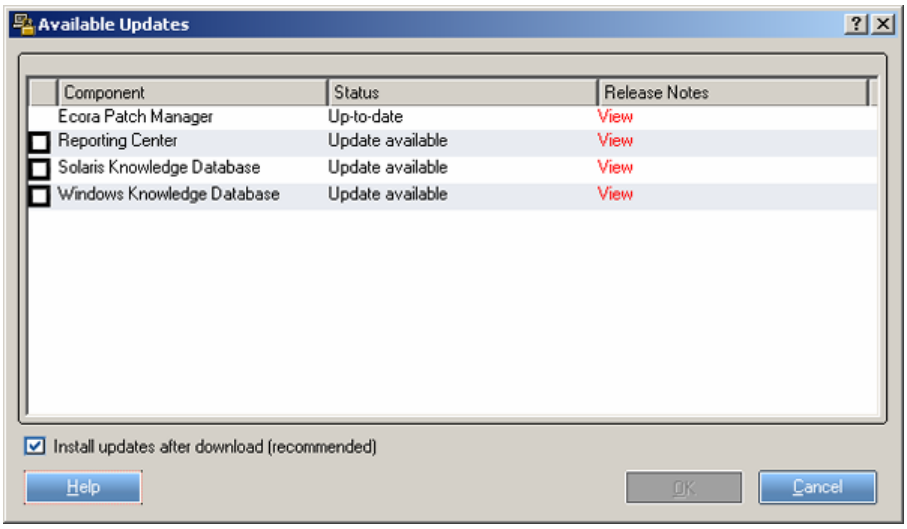

Morning Report
Task
Schedule
Settings
Scheduled Task Completed
Delete the task if it is not scheduled to run again.
Stop the task if it runs for:
72
hour(s)
0
minute(s).
Idle Time
Only start the task if the computer has been idle for at least:
minute(s)
If the computer has not been idle that long, retry for up to:
minute(s)
Stop the task if the computer ceases to be idle.
Power Management
Don't start the task if the computer is running on batteries.
Stop the task if battery mode begins.
OK
Cancel
Apply

Getting Updates

The Ecora staff is committed to continually improving the products and will make the enhancements available to customers through our website. The upgrade utility enables you to apply new software packages and new patch database content provided by Ecora.

To upgrade:

1. Run the Ecora software.
2. Click on the **Update** button (or choose **File...** **Update...**).
3. Select the component to update (Patch Manager software, Solaris Knowledge Database, Windows Knowledge Database, Reporting Center).
4. Click in the checkbox for **Install software update after download** to automatically install the update so there's no additional manual steps.
5. Click **OK**.
6. Follow the instructions to download and install.



If there has been a database structure change, you may be prompted to migrate the database.

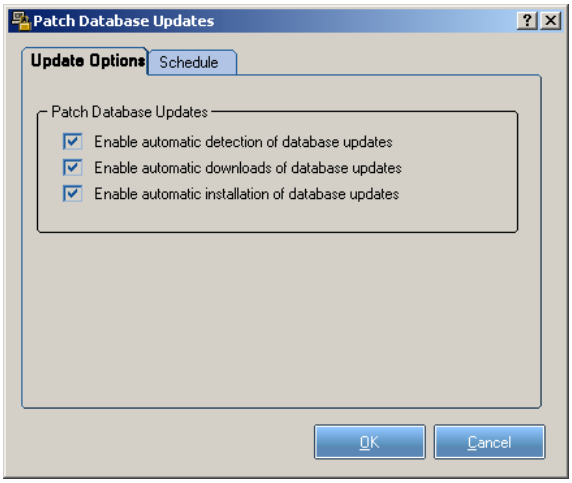
If you need to operate without Internet connectivity, refer to the instructions to update manually.

Scheduling Updates

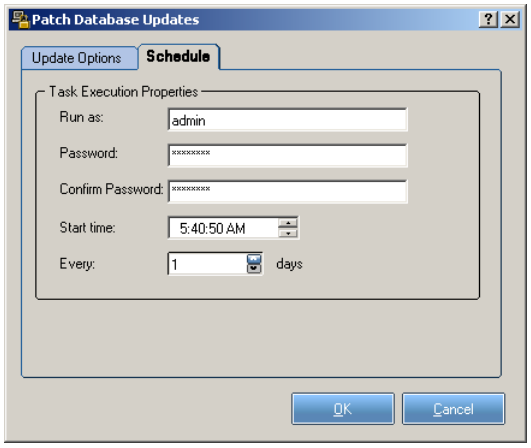
The patch information is only as current as your latest download. Ecora updates the data frequently, so scheduling regular checks is recommended.

To schedule upgrades:

1. Run the Ecora software.
2. Choose **Tools... Schedule Updates...** from the menu.
3. On the Update Options tab, enable the options **Enable automatic detection of database updates**, **Enable automatic downloads of database updates**, and/or **Enable automatic installation of database updates**.



4. On the Schedule tab, enter an administrative username in the Run As textbox and enter (and confirm) the valid password for that account.
5. Set the time of day and frequency of checks (every *n* days).
6. Click **Ok**.

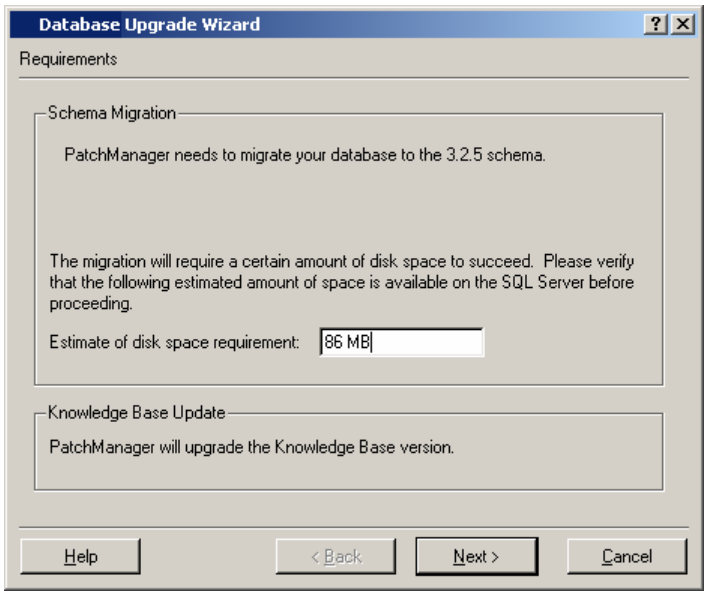


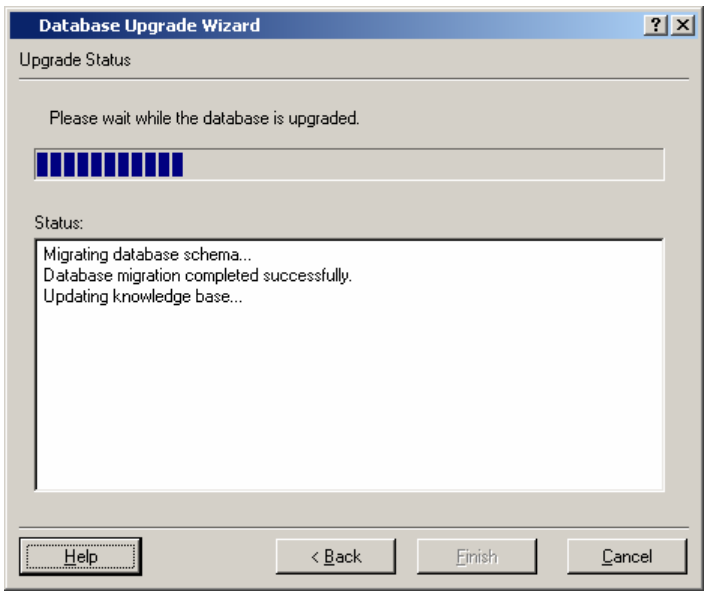
Migrating the Database

There are times when new features require a database schema change, which requires migrating existing databases to the new structure. For example, Version 4.0 adds support for agents, which requires a schema change. When a schema change is required, you are prompted to migrate your existing database to the new structure.

To migrate:

1. Upgrade the Ecora software with the latest from Ecora's website.
2. The Database Upgrade Wizard displays the estimated disk space required for the migration. Verify that adequate space is available and click **Next >**.
3. Wait while the database is migrated.
4. Click **Finish**.


Database Upgrade Wizard
Requirements
Schema Migration
PatchManager needs to migrate your database to the 3.2.5 schema.
The migration will require a certain amount of disk space to succeed. Please verify that the following estimated amount of space is available on the SQL Server before proceeding.
Estimate of disk space requirement:
86 MB
Knowledge Base Update
PatchManager will upgrade the Knowledge Base version.
Help
< Back
Next >
Cancel



Agent Installation & Setup

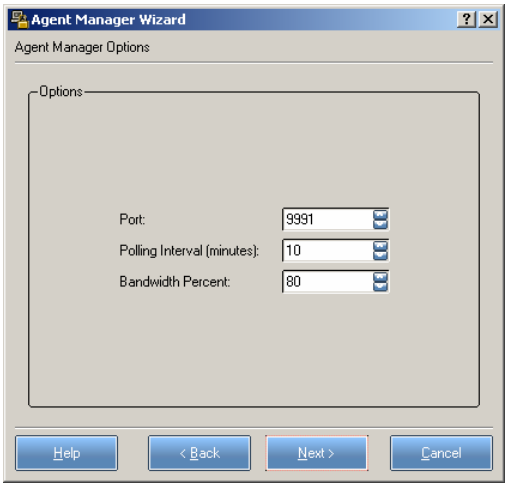
Installing the Agent Manager

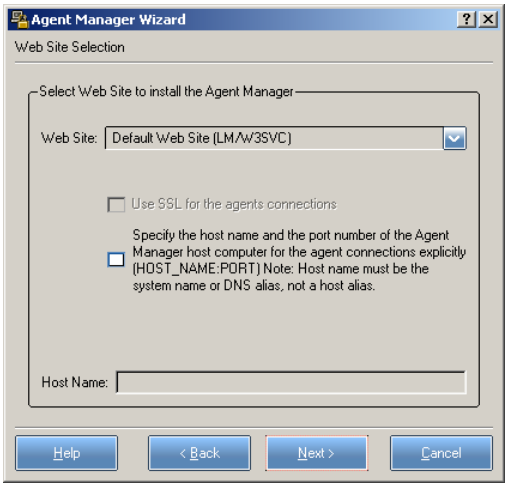
To install the Agent Manager:

1. Run Patch Manager.
2. Choose **File... Settings** from the main menu.
3. Click on the **Optional Agent** tab (which requires using the right arrow to bring the tab into view).
4. Verify that the prerequisite system requirements are met (or cancel out and go install the necessary software before returning).
   Note: Using agents causes additional system requirements.
5. Click the **Install** button. The Agent Manager Installation wizard opens.
6. Click the **Next >** button.
7. Enter the **Port Number** to be used for communication between the Agent Manager and Patch Manager.
8. Enter the **Polling Interval**, which is the number of minutes between each contact with agents.
9. Enter the **Bandwidth Percent**, which is the maximum percentage of network bandwidth agent communication may consume.
10. Click **Next >**.
11. Select the website from the drop-down list.
12. Choose to **Use SSL...** or **Specify host name and port number...** for agent communication.
13. If you chose to specify host name and port number, enter them in the text box separated by a colon.
14. Click **Next >**.
15. Click **Finish**.

For information on agent manager installation, see Troubleshooting; Optional Agent.

Agent Manager Wizard
Welcome
Welcome to the Agent Manager installation wizard. This wizard will help you install the Ecora Agent Manager on your system. The Agent Manager will allow you to deploy agents to systems on your network and perform all Patch Manager operations through these agents.
Click Next to start the Agent Manager installation.
Help
Next >
Cancel



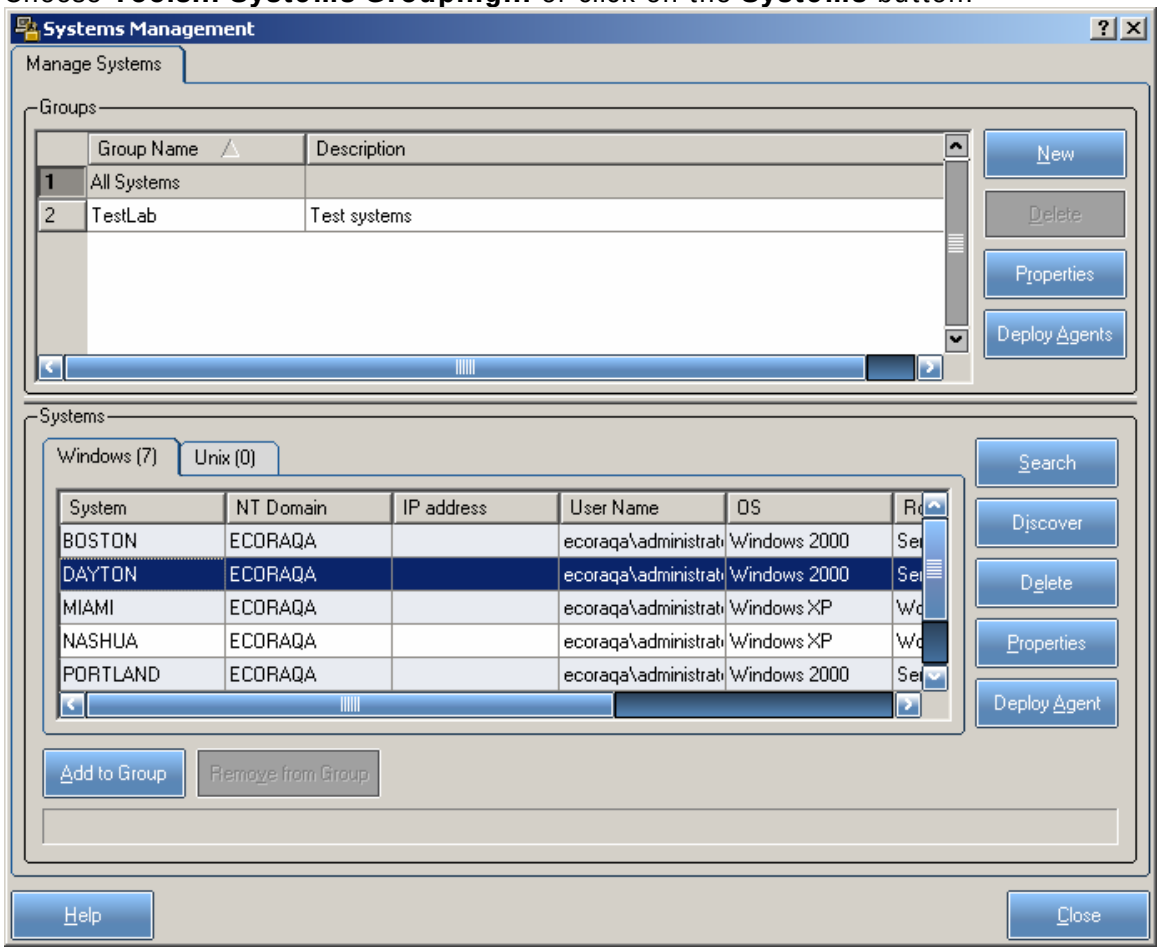

Agent Manager Wizard
Web Site Selection
Select Web Site to install the Agent Manager
Web Site:
Default Web Site (LM/W3SVC)
Use SSL for the agents connections
Specify the host name and the port number of the Agent Manager host computer for the agent connections explicitly (HOST_NAME:PORT) Note: Host name must be the system name or DNS alias, not a host alias.
Host Name:
Help
< Back
Next >
Cancel

Installing Agents

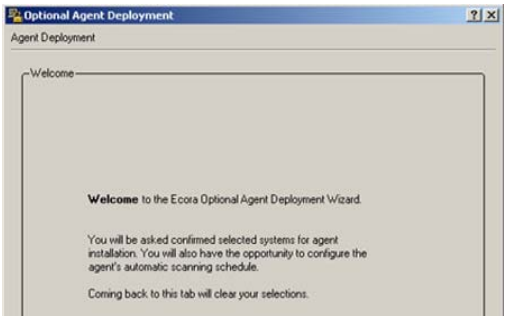
Agent software is installed on target systems through a deployment process in the Systems Management interface.

To deploy the agent to systems:

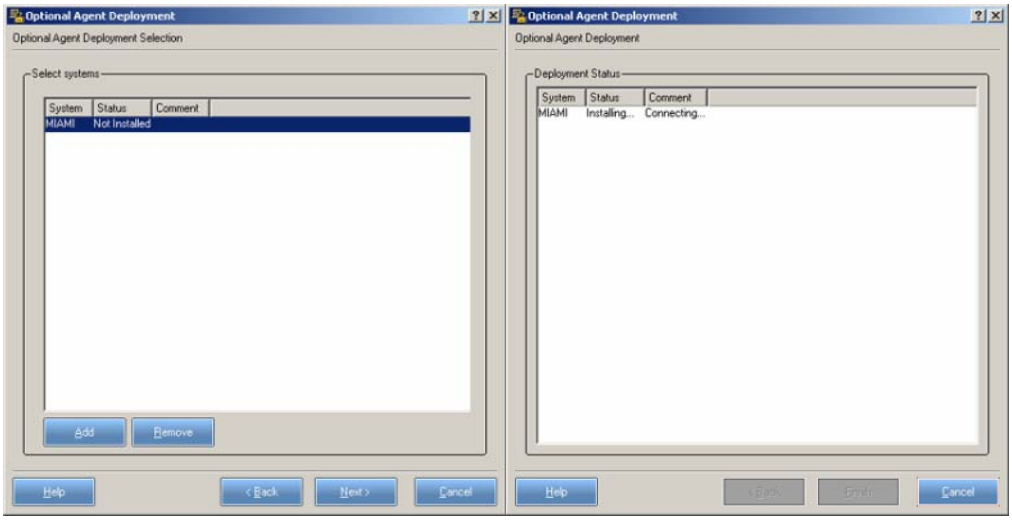
1. Choose **Tools... Systems Grouping...** or click on the **Systems** button.



2. If all the systems you wish to involve are listed, proceed to the next step. If not, click **Discover...** and locate additional systems on which to deploy agents.
3. Select the systems (or groups of systems) on which you wish to install the agent software.


Optional Agent Deployment
Agent Deployment
Welcome
Welcome to the Ecora Optional Agent Deployment Wizard.
You will be asked confirmed selected systems for agent installation. You will also have the opportunity to configure the agent's automatic scanning schedule.
Coming back to this tab will clear your selections.

4. Click the **Deploy Agent** button.
5. Click **Next >**.
6. Confirm, **Add**, or **Remove** systems from the list selected for agent deployment and click **Next >**.
7. Once installation is confirmed, click **Finish**.



For instructions on manual agent installation, see [Troubleshooting; Optional Agent](#).

Agent Management

Version 4.0 introduces the additional capability in Ecora Patch Manager to deploys a software "agent" package to systems which communicates with a server for patch installation and system analysis. This architecture is called the Optional Agent Manager and uses the Patch Manager console as the master server and installs agent software on client systems that need patch management services. The optional agent solution provides the flexibility to effectively handle hardened devices and systems connected to the network inconsistently.

The following are concepts and definitions apply:

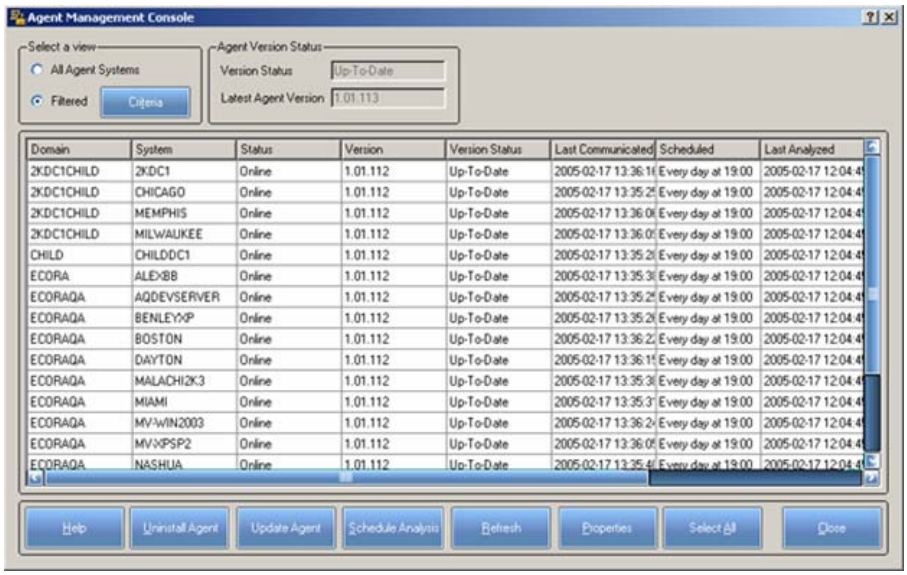
- Agent Manager - the server component of the agent communication that directs and synchronizes agent activities
- Agent - the software installed on target or client systems that will communicate with the server
- OAService - the software module responsible for job generation and workflow management
- Data Processor - the software module responsible for executing jobs related to the database (saving analysis to database or extracting knowledge from the database)

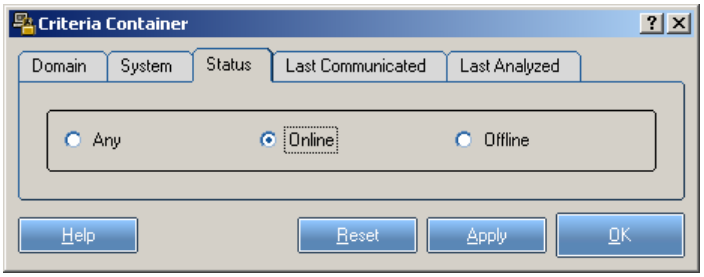
See a diagram of Patch Manager connections and access requirements.

Agent Manager Console

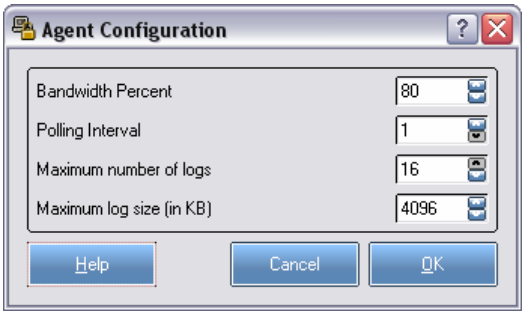
To access the Agent Manager Console:

1. Choose **Tools... Agents...** or click on the **Agent** button.
2. In the Select a view group (upper left side of dialog), select to display **All Agent Systems** or a **Filtered** view.
3. Click **Criteria** to set the values and operators for the filter (such as name matching, on/offline status, last contact).
4. Review the data about deployed agents, including sortable columns for each agent's Domain, System, Status, Version, Version Status, Last Communicated (timestamp), Scheduled (patch analysis scheduled time), Last Analyzed (timestamp), Last IP address, Polling Interval (in minutes), and Bandwidth Percentage.





5. Click **Un/install Agent...** to start the wizard to remove the agent from the selected system.
6. Click **Schedule Analysis...** to set the frequency, start date, and time for automatic analysis on a recurring basis.
7. Click **Refresh** to update the displayed information.
8. Click **Properties...** to review or edit the selected agent's settings (bandwidth, polling, logs).
9. Click **Close**.

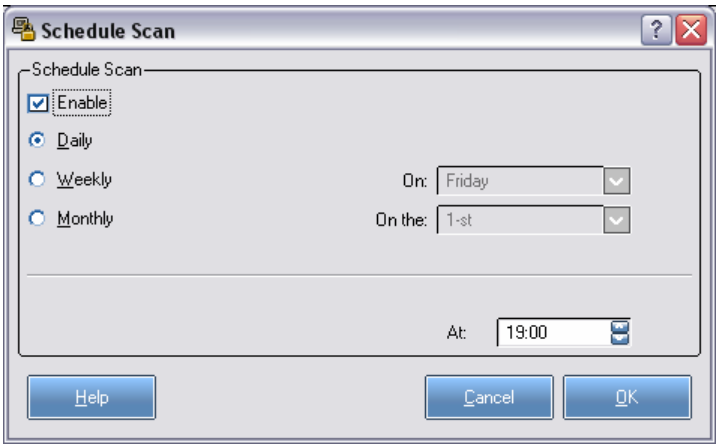


Scheduling Analysis for Agents

To schedule ongoing agent analysis:

Tip: The following instructions set up recurring scans, but you can also schedule scans as non-agent systems are scheduled; see Scheduling Analysis.

1. Choose **Tools... Agents...** or click on the **Agent** button.
2. Locate and select the agent you wish to schedule.
3. Click the **Schedule Analysis...** button and set the frequency for automatic analysis on a recurring basis.
4. Click in the checkbox to **Enable** scheduled analysis.
5. Choose **Daily**, **Weekly**, or **Monthly** for the frequency of automatic analysis.
6. Set the start date, day, and/or time for recurring scans.
7. Click **OK**.

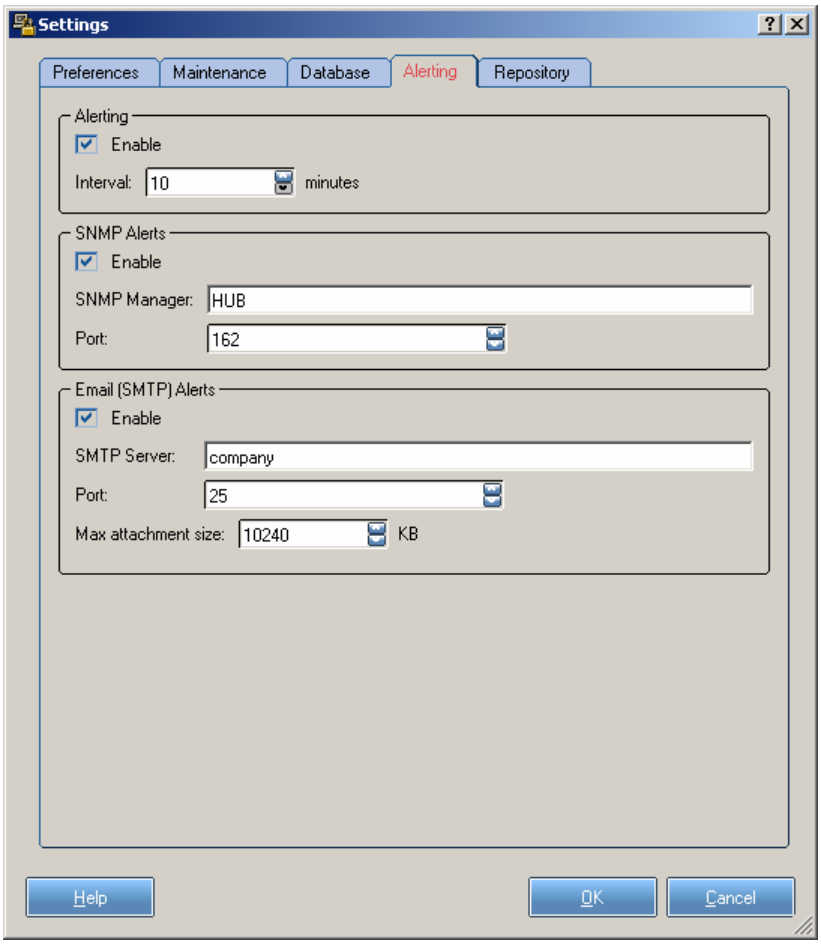


Using Alerts & Triggers

Triggers and alert allow you to define conditions that result in actions. For example, you may choose to establish a trigger condition for a new patch or an analysis failure, then add an alert in the form of email notification if that condition (trigger) is met.

To configure the software for triggers & alerts:

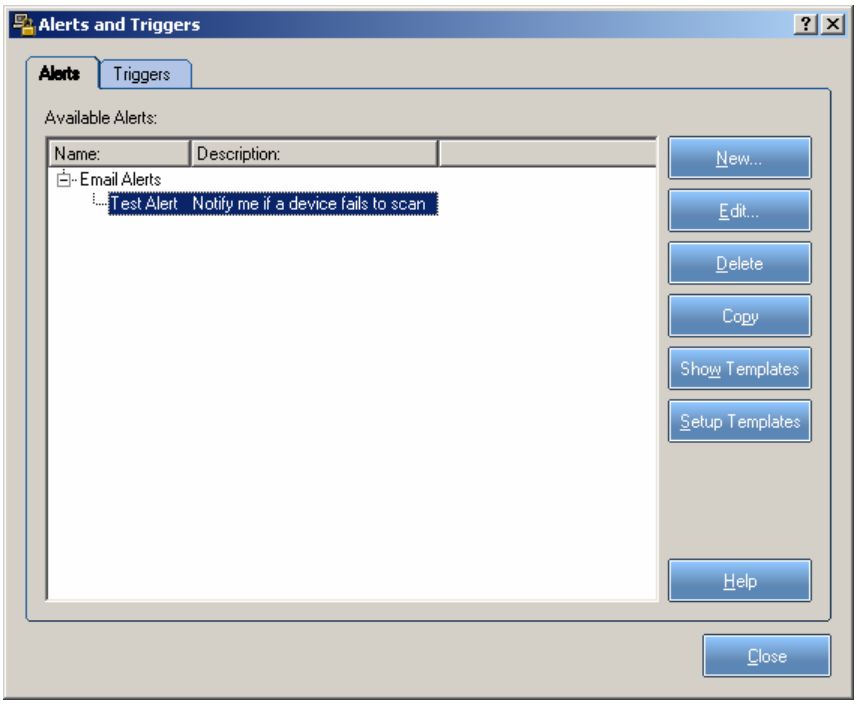
1. Run the Ecora software.
2. Choose **File... Settings...** from the menu.
3. Click on the **Alerting** tab.
4. In the Monitoring area, click in the **Enable** checkbox to enable monitoring.
5. Use the drop-down list to select an interval (in minutes- minimum 10 minutes) to set how often the software checks for the conditions you define.
6. In the SNMP Alerts area, click in the **Enable** checkbox to enable alerts via SNMP traps.
7. Enter the SNMP Manager name and Port number. The SNMP Manager can be the name of any server running an application capable of receiving SNMP traps.
8. In the Email (SMTP) Alerts area, click in the **Enable** checkbox to enable alerts via email.

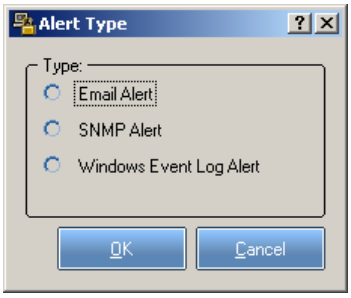


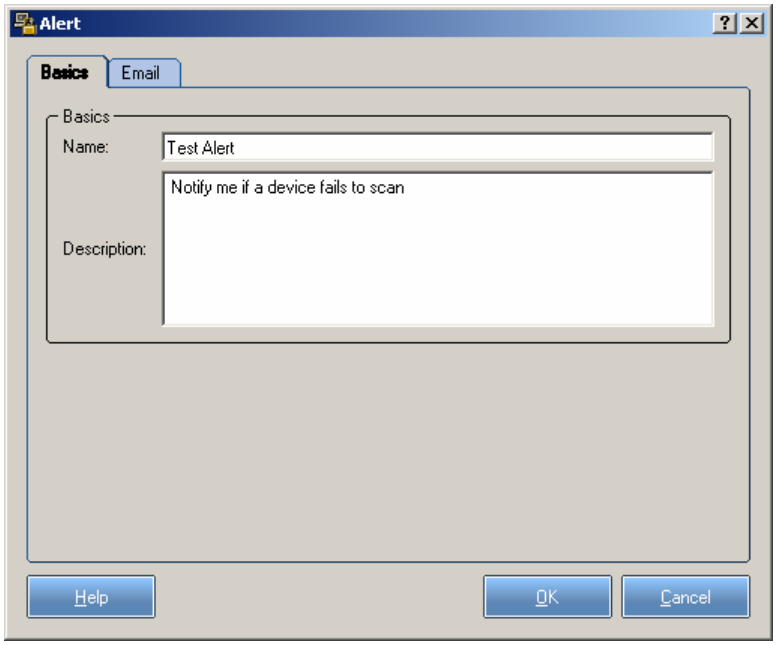
9. Enter the SMTP Server name, Port number, and the Maximum Attachment Size (reports can get large), and a list of email recipients' email addresses.
   Tip: The SMTP Server is generally your mail server in fully qualified domain name (FQDN) format (server-name.domain-name.nnn) or by full IP address.
10. Click in the checkbox to **Enable Triggers created from templates** if you wish to use provided triggers as editable examples.
11. Click **OK**.

To create an alert:

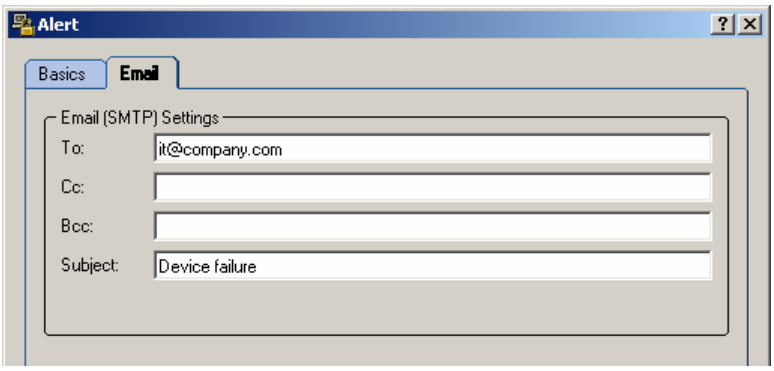
1. Run the software.
2. Choose **Edit... Alerts and Triggers...** from the main menu.
3. Click **New...**.
4. Click in the radio button for the type of alert you wish to set.
   An **Email Alert** allows you to specify an email message to be sent when the trigger condition is met.
   An **SNMP Alert** can send a message to the manager console.
   A **Windows Log Event Alert** writes information, errors, +/or warnings to the Windows event log.
5. Click **OK**.
6. Enter a name and description for the alert.
7. Proceed according to the type of alert you selected.



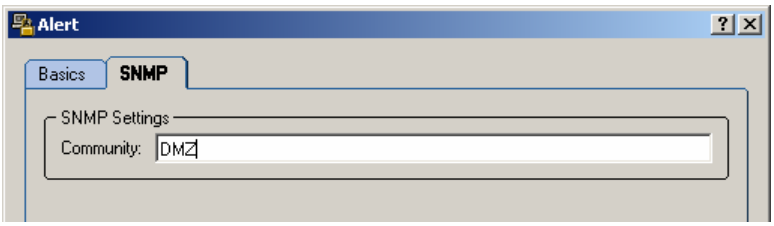




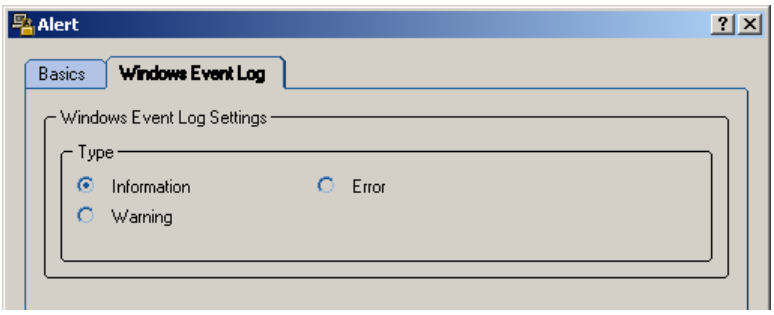
7. Click on the **Email** tab.
8. Enter the email addresses for those you wish to receive the report and the subject line of the email.
9. Click **OK**.



7. Click on the **SNMP** tab.
8. Enter the community server acting as your SNMP server. SNMP global settings are located under **File... Settings... Alerts** tab.
9. Click **OK**.

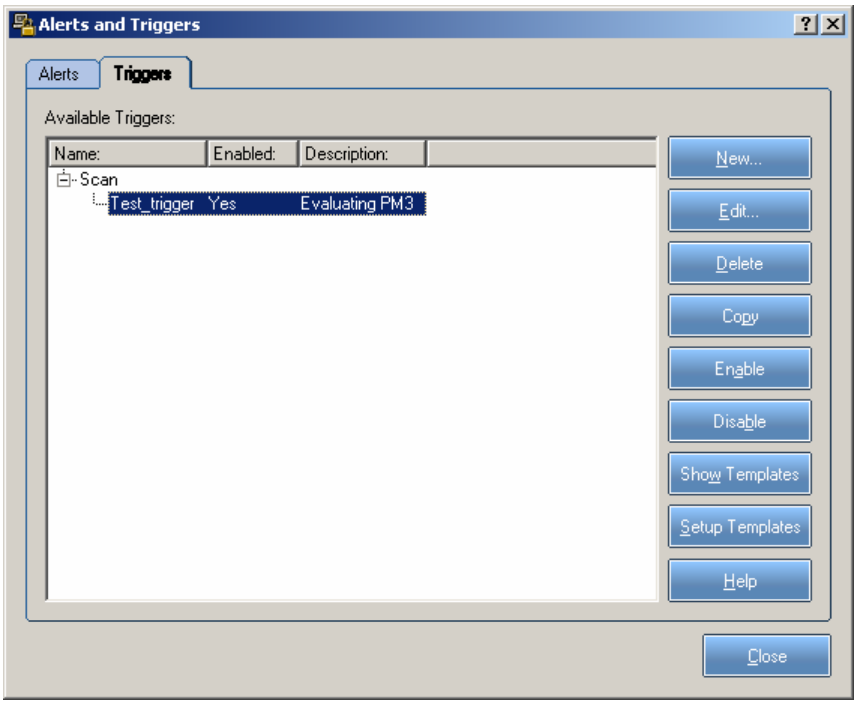


7. Click on the **Windows Log Event** tab.
8. Enter the computer name of the machine whose log will record events (if left blank, the software writes to the machine where the Ecora software is installed).
9. Click in the **Information**, **Warning**, **Error**, or **Success** radio button to indicate which event types will be written to the Windows event log.
10. Click **OK**.

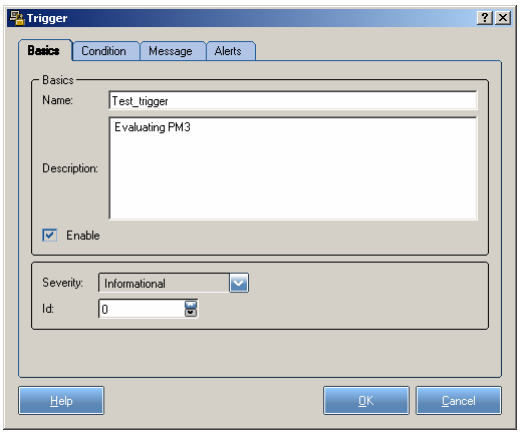


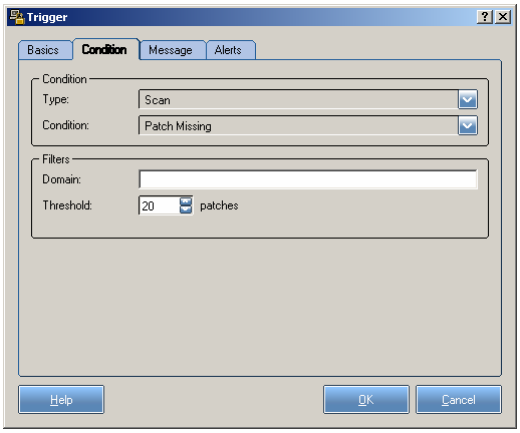
To create a trigger:

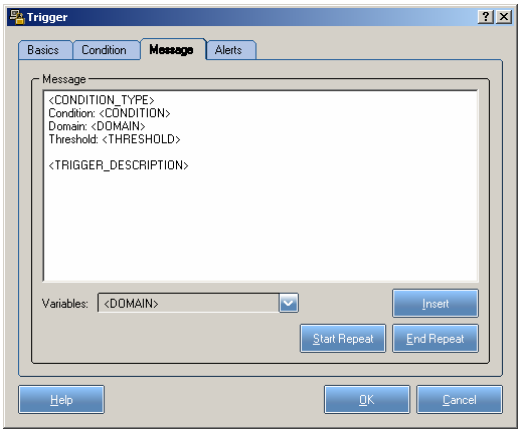
1. Choose **Edit... Alerts and Triggers...** from the main menu.
2. Click on the **Triggers** tab.
3. Click **New...** (or select an existing trigger and click **Edit...**).
4. On the Basics tab, enter a **Name** and **Description** for the trigger.

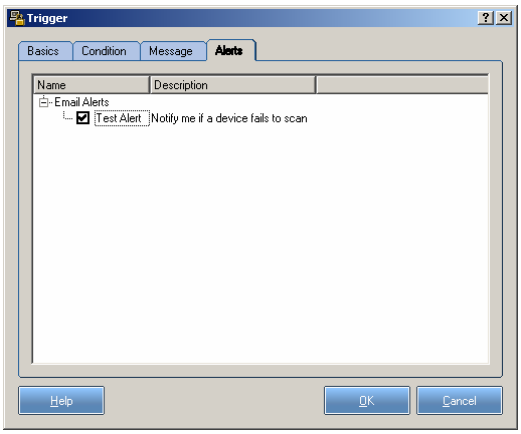


5. Verify that the **Enable** option is checked.
6. Use the drop-down list box to select the **Severity** level.
7. Use the drop-down list box to select the **ID**.
8. Click on the **Conditions** tab.
9. Click in each relevant product module checkbox.
10. Use the drop-down list box to select the **Type** (Scan, Push, Patch Database Update).
11. Use the drop-down list box to select the **Condition** (Patch Missing, Scan Failure, Database Age; Push Failure; New Patches, Database Update Exist, Update Detection Failure, Download Failure, Download Success, Installation Failure, Installation Success,).
12. Set the Filters according to the prior selections.
13. Click on the **Message** tab.
14. Enter the **Message** name.
15. Enter the message body in the text box, using the drop-down to select variables and **Insert** button to include them in the message.
16. Use **Start Repeat** and **Stop Repeat** buttons to create lists within the message.
17. Click on the **Alerts** tab.
18. Use the expandable tree to locate the alert(s) you would like to use.
19. Click in the checkbox for the alert(s) you wish to associate with this trigger.
20. Click **OK** to save the defined trigger.







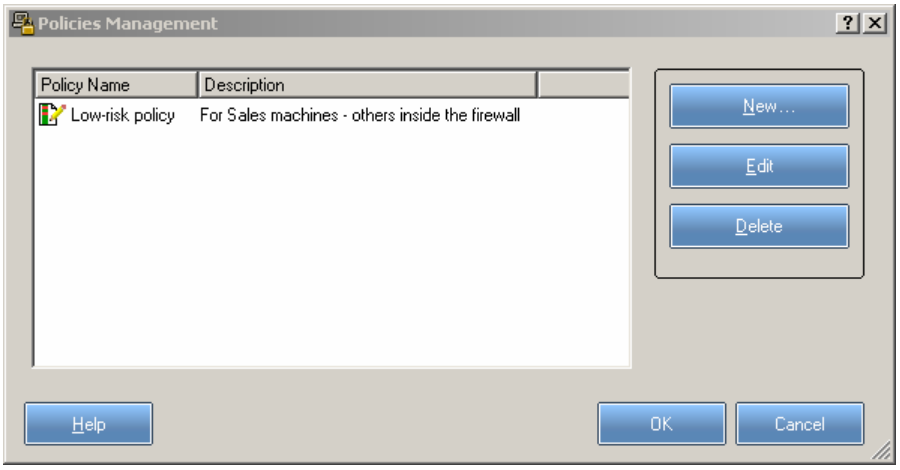


Policy Management

Policies allow you to create generalized rules about how you want systems in your environment configured (presumably secured to the latest critical patches). You may choose to prioritize certain groups for stricter policies for applications you consider higher risk. Policies allow you to define these rules, apply them to groups you create, then schedule scans to ensure that you're always aware of systems that do not comply with your policies.

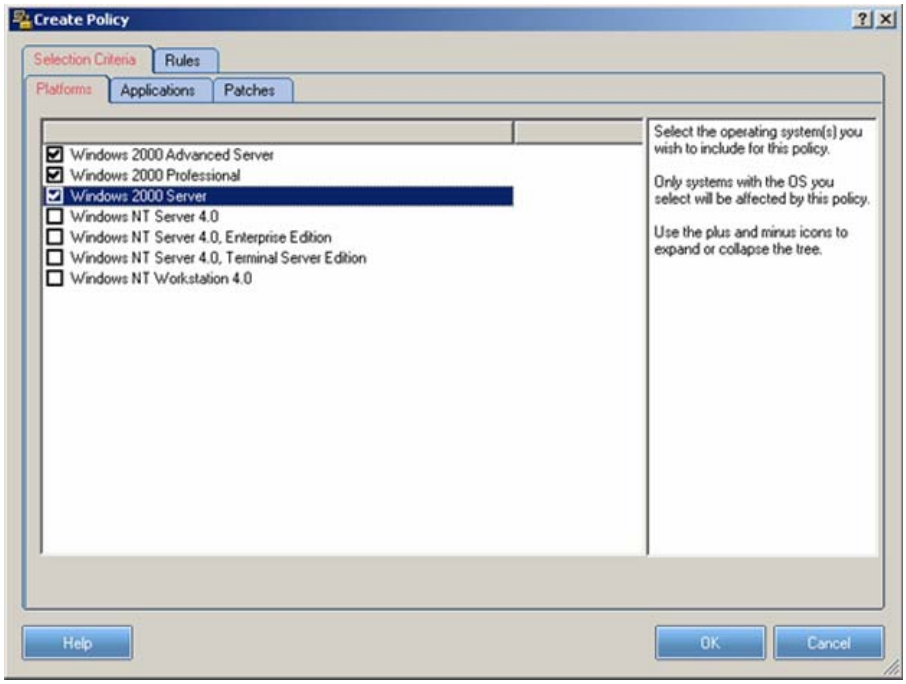
Creating Policies

1. Choose **Tools... Policy Management...** from the menu.
2. Click the **New...** button to access a dialog for creating a policy.
3. Enter a name and description for the new policy and click **OK**.
4. In the Create Policy dialog box, the Selection Criteria tab, click on the **Platforms** tab.

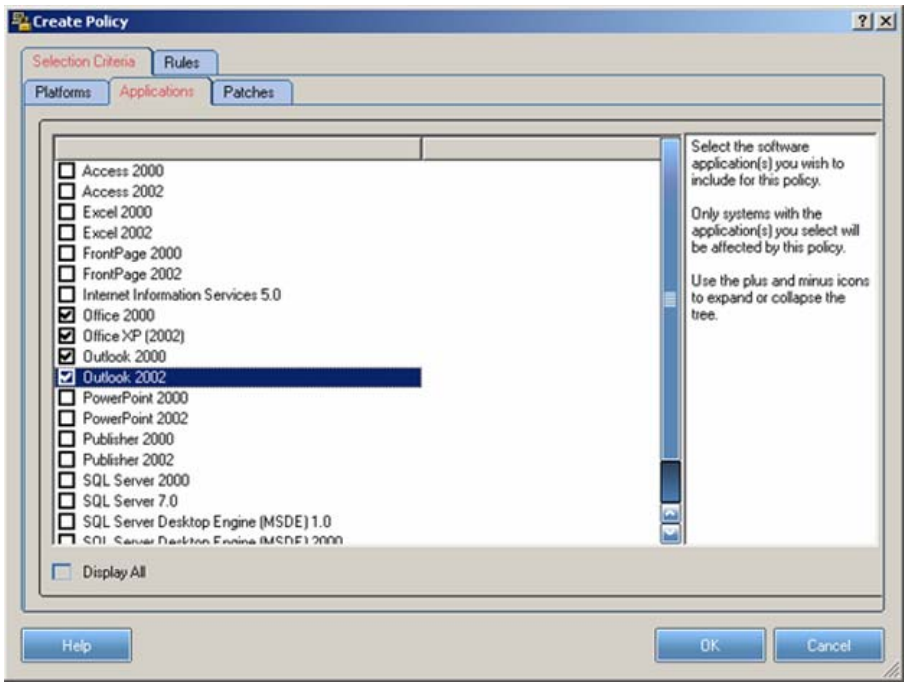


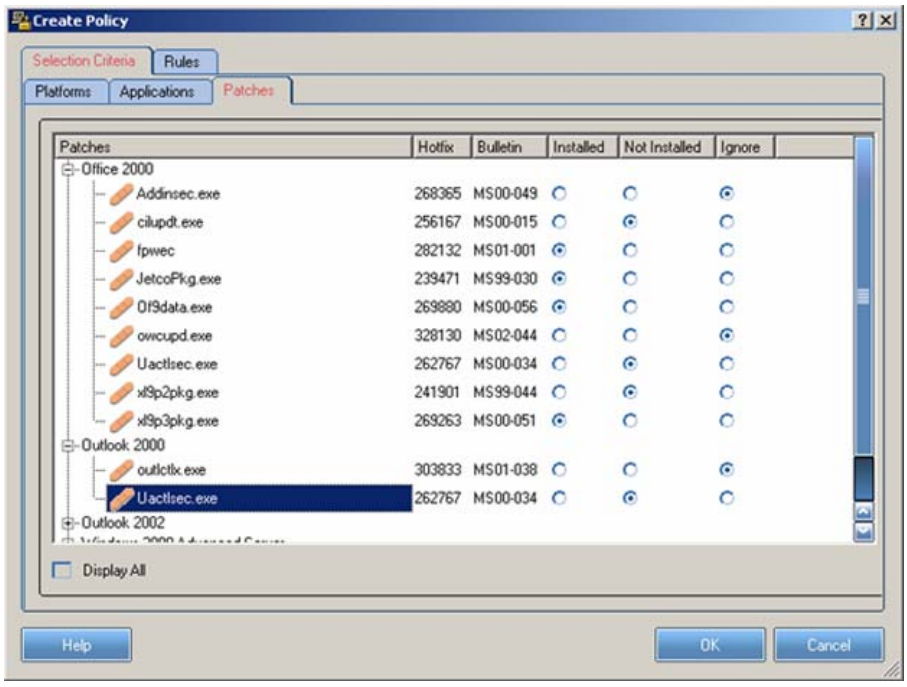
5. For every OS version to which this policy will apply, click in the checkbox or choose **Display All**.

   Tips: Make selections that share patches for best results.

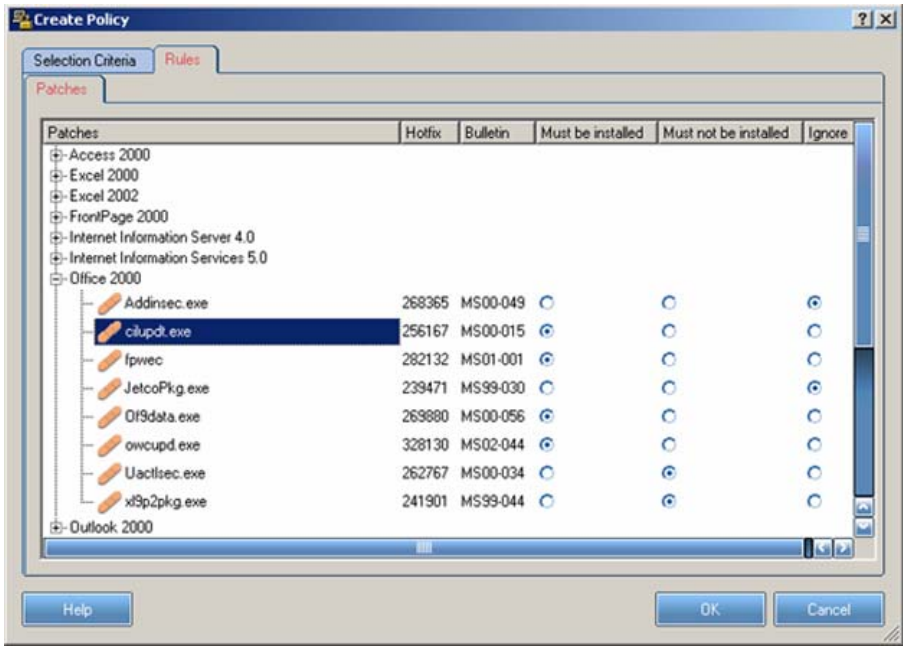

Create Policy
Selection Criteria
Rules
Platforms
Applications
Patches
Windows 2000 Advanced Server
Windows 2000 Professional
Windows 2000 Server
Windows NT Server 4.0
Windows NT Server 4.0, Enterprise Edition
Windows NT Server 4.0, Terminal Server Edition
Windows NT Workstation 4.0
Select the operating system(s) you wish to include for this policy.
Only systems with the OS you select will be affected by this policy.
Use the plus and minus icons to expand or collapse the tree.
Help
OK
Cancel

6. Click on the **Applications** tab.
7. For every software application to which this policy will apply, click in the checkbox.
8. Click on the **Patches** tab.
9. Click on plus signs to expand the tree by application to see patches.
10. For relevant patches, click in a radio button - **Installed**, **Not Installed**, **Ignore**. This controls which systems will be displayed in Policy view - only systems with patches that meet the criteria will show in the report. For example, leaving a patch set to **Ignore** will display systems with the patch installed OR not installed.





11. Click on the **Rules** tab.

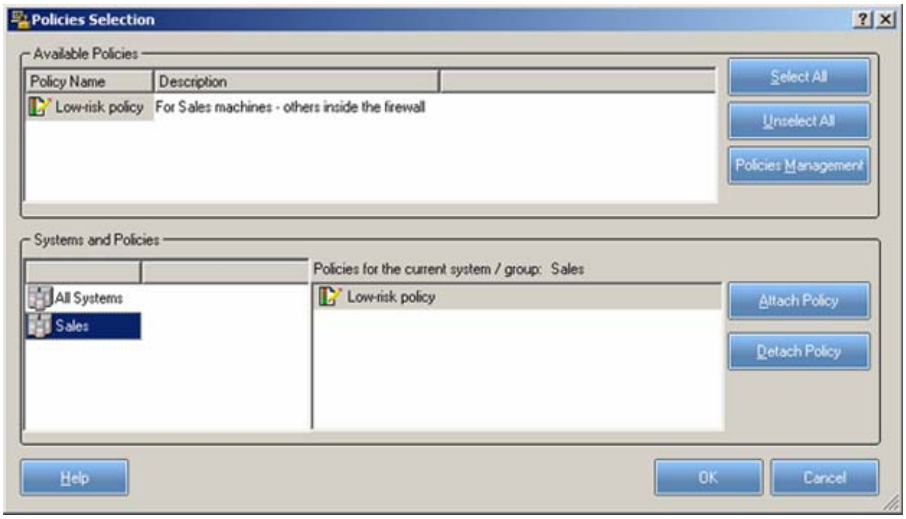


Tips: You do not have to define criteria on all three tabs. If you DO: the filtering queries combine as follows: For platforms, the relationship is OR; for applications, the relationship is AND; and for patches, the relationship is AND. Policies work like IF/THEN statements. IF the selection criteria is true, THEN the rule is checked for true/false to judge compliance.

12. Click on plus signs to expand the tree by application to see patches.
13. For relevant patches, click in a radio button - **Must be Installed**, **Must Not be Installed**, **Ignore**. This controls which systems will be considered compliant with the policy.
14. Click **OK** to close the policy editor.
15. Click **OK** to close the policy manager.
16. Click **Yes** to apply the policy to systems or groups at this time.

Applying Policies to Systems and Groups

1. Choose **Tools... Policies Selection...** from the menu.
2. Select a policy in the upper pane to be applied to a group in the lower pane.

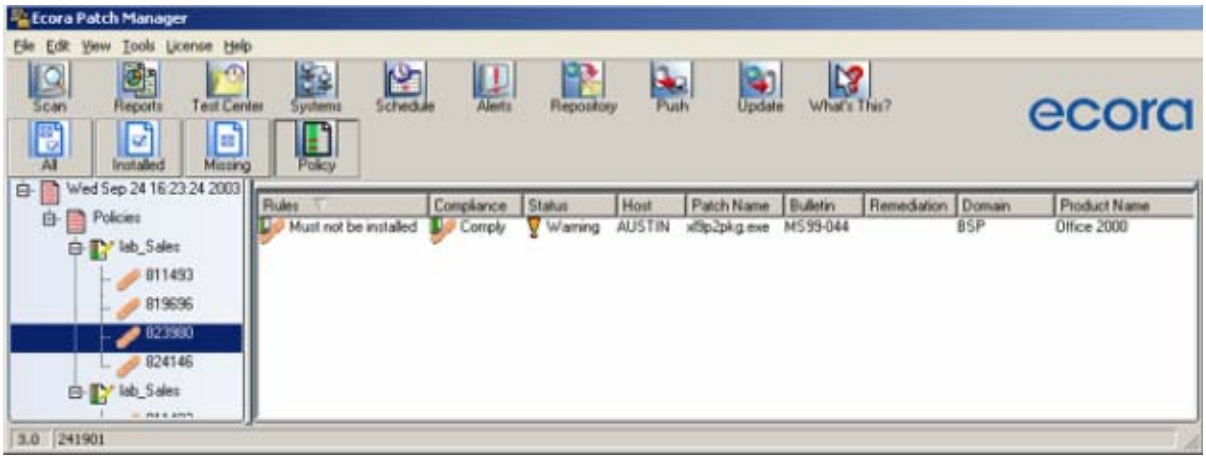


Tips:
If you have no policies defined, click on **Policies Management** and follow the policy creation instructions above. If you have no groups defined, click on **System Management** and follow the grouping instructions.

3. Select a group in the lower pane to which to apply the selected policy.
4. Click on the **Attach Policy** button to apply the selected policy to the selected group.
5. Click **OK**.

Viewing by Policy Compliance

1. Follow the instructions for creating and applying policies above.
2. Follow the instructions for scanning systems.
3. In the main interface window **Views** bar, select the **Policy** button.
4. Navigate the interface as usual, using the tabs to narrow your view.



Remediation by Policy

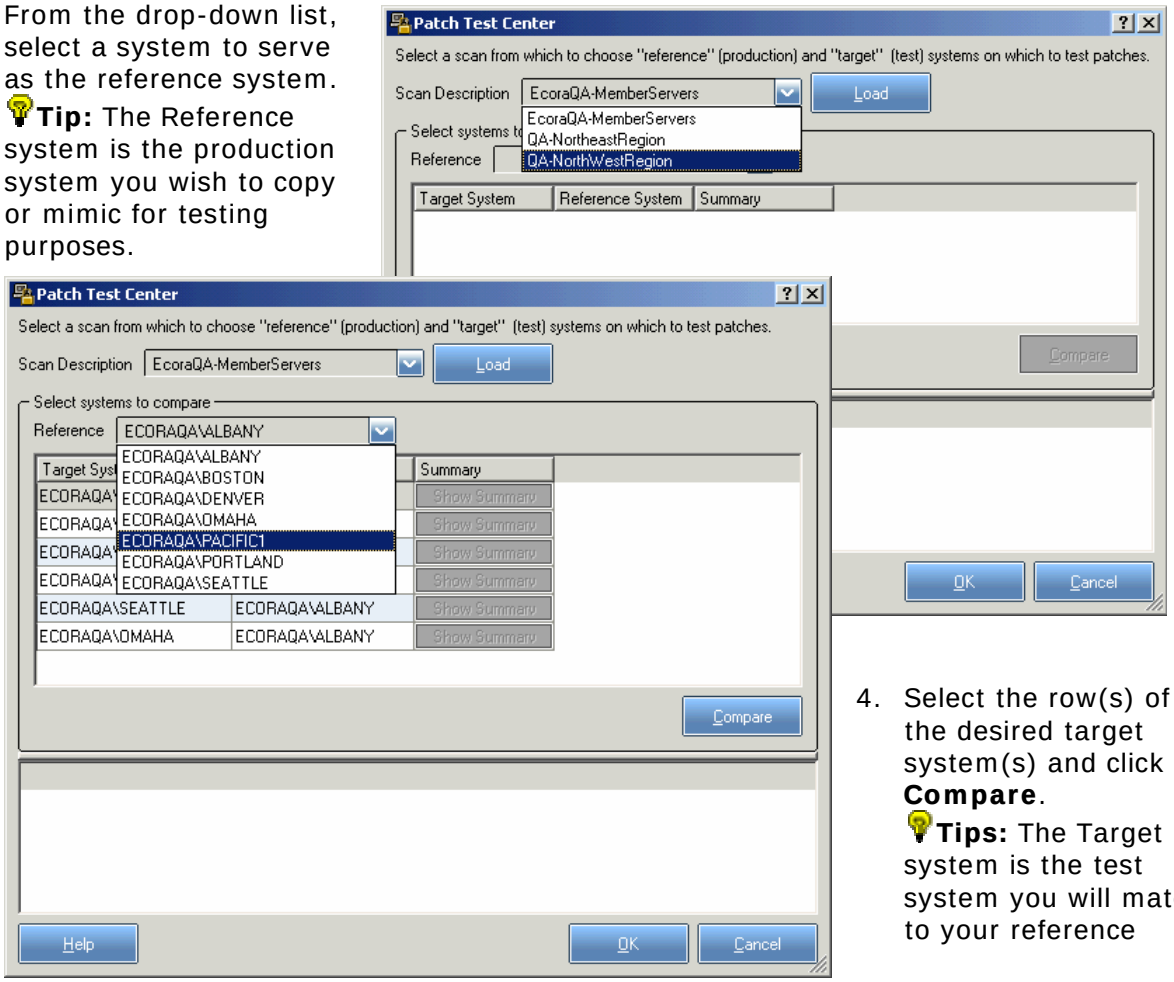
1. Follow the instructions for creating and applying policies above.
2. Follow the instructions for scanning systems.
3. In the main interface window **Views** bar, select the **Policy** button.
4. In the left pane, select the **Policy** tab.
5. Navigate to the Policy level of the tree and select the policy for which you want automatic remediation.
6. In the right pane, click in the checkbox for Remediation.
7. Click the **Push** button and follow the instructions for creating a push task.

Patch Test Center

Patches should always be tested in a lab or on a test machine prior to being deployed on production machines where problems and conflicts might impact your business operations. The Test Center feature allows you to choose a system in your environment to act as a model or "reference" that you can compare other systems against and use to test patches BEFORE releasing them to production.

There are two general uses for the Test Center.
Case 1: You can use the Test Center to remediate one or more target systems to match a reference "gold standard" system. You can use this to replicate a configuration or "bulk patch" a system to a proven standard.
Case 2: You can choose a model production system as the reference (perhaps one of a group of systems configured consistently, such as one of ~50 sales machines), then choose a system within your test lab as the target and remediate it to match exactly (both patching and rolling back as necessary). Maintain the test system and use it to install, test, and verify proper function of all patches and service packs before deploying to production systems.

1. Click on the **Test Center** button (or choose **Tools... Test Center...** from the menu or press F9).
2. From the Scan Description drop-down list, select a saved analysis and click **Load**.
3. From the drop-down list, select a system to serve as the reference system.
   Tip: The Reference system is the production system you wish to copy or mimic for testing purposes.

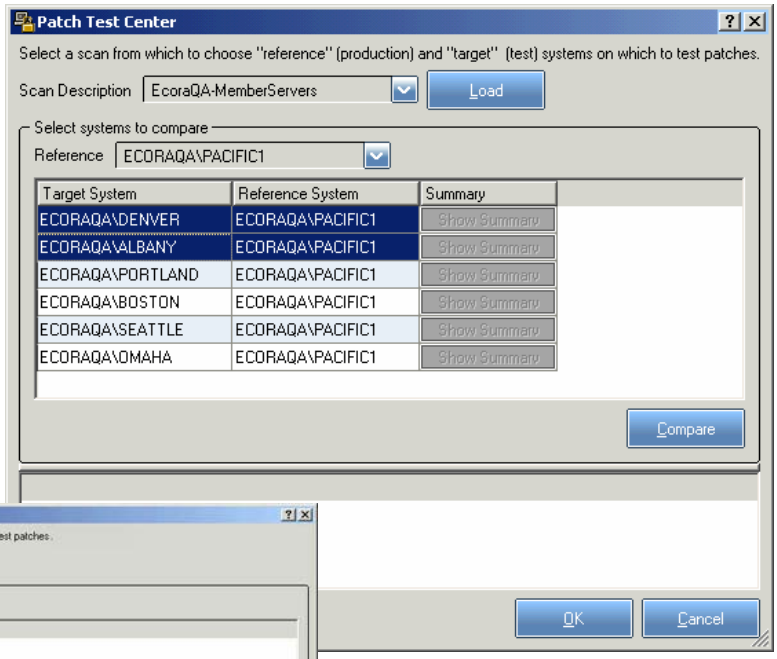


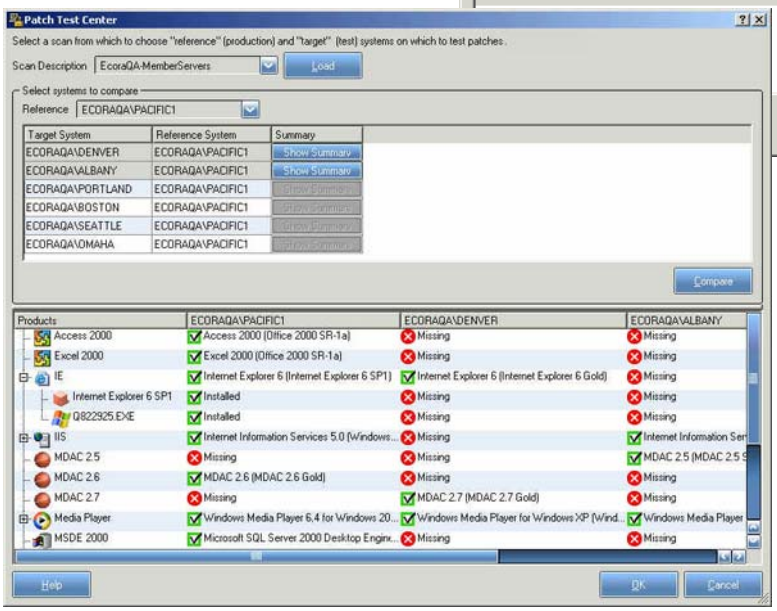
4. Select the row(s) of the desired target system(s) and click **Compare**.
   Tips: The Target system is the test system you will match to your reference

system and use to test patches and hotfixes.
For an overview that baselines the reference against multiple target systems, use the CTRL or SHIFT keys to select multiple rows before comparing.

5. Use the lower pane to compare the reference to the target(s) by product.

6. When you are ready for a detailed comparison of two systems, click **Show Summary** in one of the rows above.

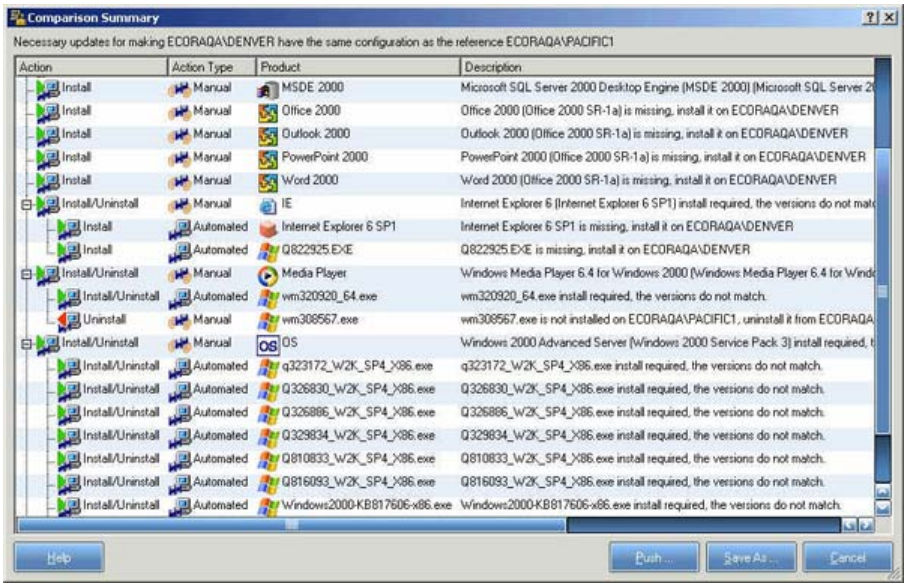




7. Use the plus signs to expand and the column headings to sort the results.

   Tip: Items marked install/uninstall indicate that the version mismatch requires a user decision on which will be standard.

8. If you wish to match the reference and target systems according to the summary, click **Push...** (and follow the instructions for installing patches).



9. If you wish to write the summary out to an HTML file, click **Save As...**.

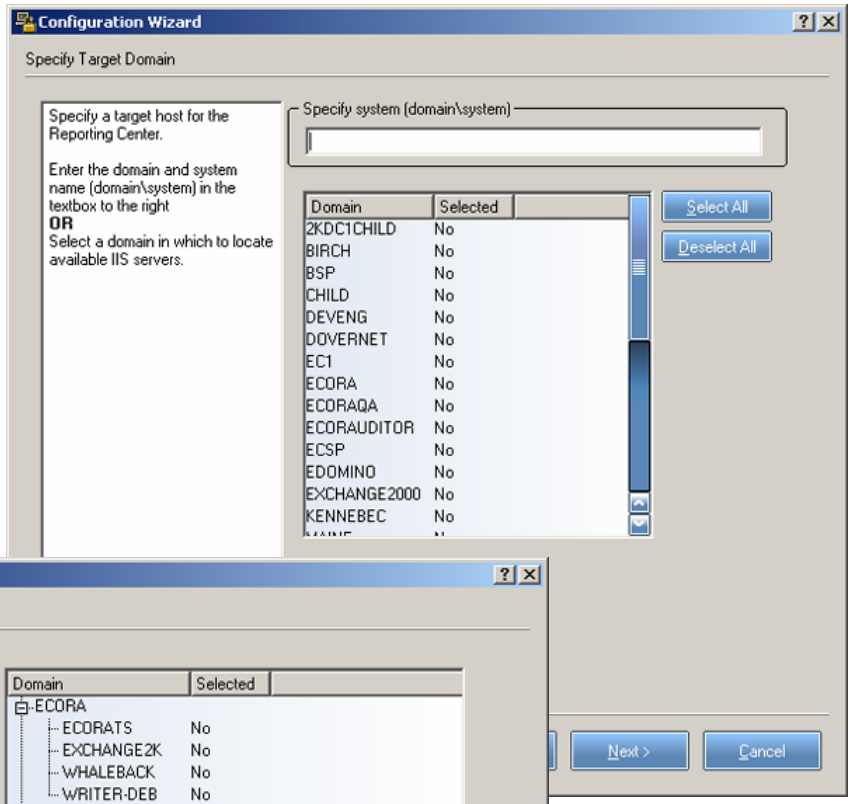
10. Click **Cancel** to close the Summary and **OK** to close the Test Center dialog.

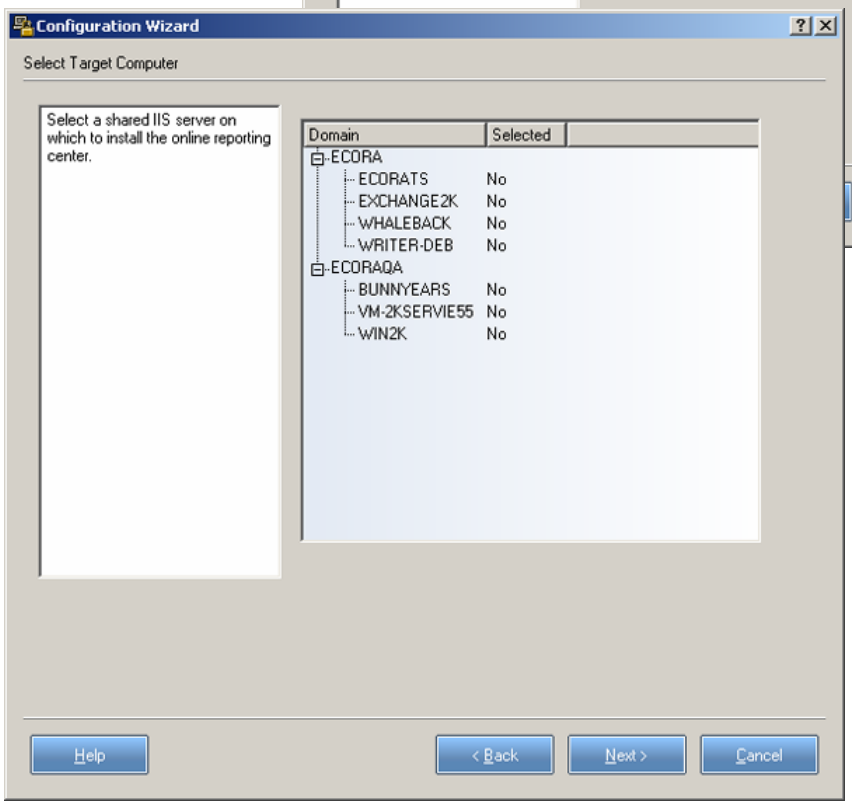
Reporting Center

The reporting center is a website interface created by Ecora to provide an intuitive way to query the Patch Manager database. The URL can be accessible to anyone in an environment who can access the share on which you choose to install the reporting center. CIOs or auditors can see a report of Hardware Inventory of the environment, whereas an IT staff member might be more interested in the Patch History report for one machine.

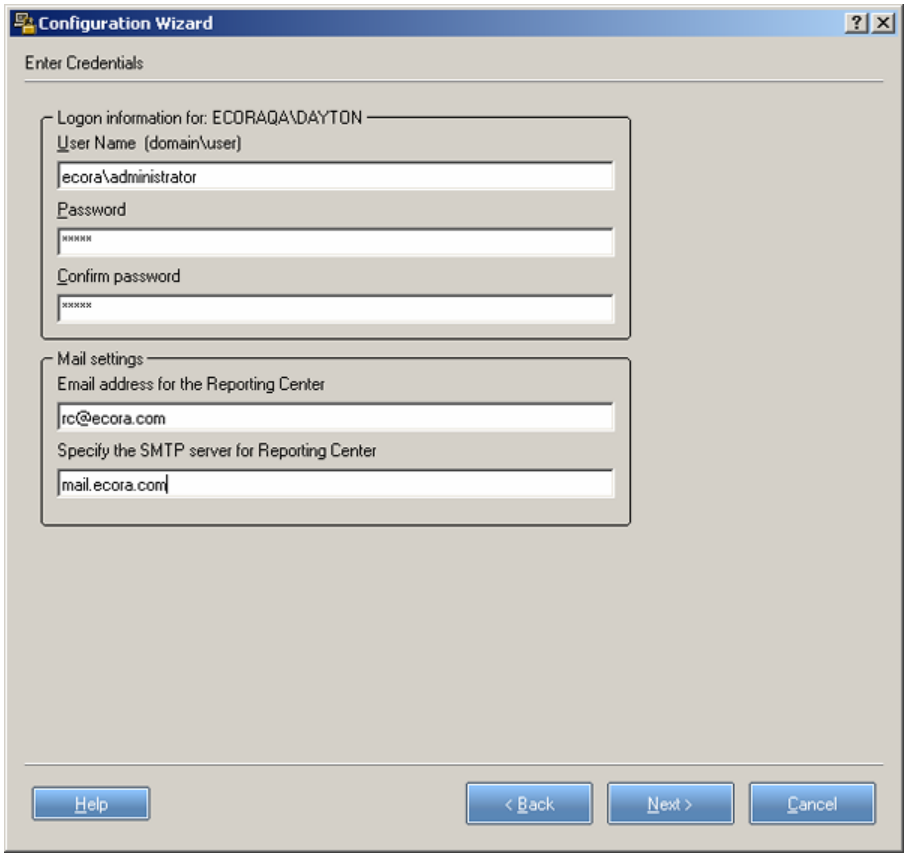
Installing the Reporting Center

1. The Configuration Wizard can be accessed via setup or **File... Settings... Reporting Center** tab.
2. Specify the target host (shared, with IIS and Microsoft .Net Framework installed).
3. Enter the domain and system in the textbox -OR- select a domain from the list to discover systems, then select a system from the resulting list.





4. Click **Next >**.
5. Enter valid credentials for accessing the target host.



6. Enter an email address from which reports will be sent.
7. Enter a valid SMTP server for mail exchange.
8. Click **Next >**.
9. Click **Finish** after confirming successful installation.

Tip: The Reporting Center is located at URL: shared_system_name/EcoraReportingCenter; where "shared_system_name" is the server where you installed it during setup - a server with IIS and Microsoft .Net.

Using the Reporting Center

1. Access the online reporting center.
   Tip: The Reporting Center is located at URL: shared_system_name/EcoraReportingCenter; where "shared_system_name" is the server where you installed it during setup - a server with IIS and Microsoft.Net.
2. If prompted, select or enter your login, enter your password, and click **OK**.
3. Select the report you want from the drop-down list. (Use the down arrow to expand a group.)
4. Click in the checkbox for the group of systems you wish to report.
5. Select other applicable options (displayed based on report selected).

Reporting Center - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://ecora/ecoraReportingCenter/
Go Links SnagIt
ecora Reporting Center
Printable Version E-Mail Report...
Export Report to CSV format...
Export Report to DOC format...
ECORAQA\Administrator
Select Report
Missing Patches
Report For All Products
Computer Groups
All Systems
Clear Selections Go
Administration
Automatically document, analyze, and fortify your IT infrastructure!
Ecora Patch Manager helps secure your systems from vulnerabilities, but that's only half the battle.
Are you regularly tracking
Done
Reporting Center - Microsoft Internet Explorer
Select Report
Missing Patches Summary
Computer Groups
All Systems
Clear Selections Go
Administration
ECORAQA\ALBANY IP Address: ; Operating System: Windows 2000 Server
Missing 'Internet Explorer 5.01' Patches - 70% - 3 out of 10 patches installed
Missing 'Internet Information Services 5.0' Patches - 100% - 0 out of 2 patches installed
Missing 'Windows 2000 Server' Patches - 50% - 17 out of 34 patches installed
Missing 'Windows Media Player 6.4 for Windows 2000' Patches - 20% - 4 out of 5 patches installed
ECORAQA\BOSTON IP Address: ; Operating System: Windows 2000 Server
Missing 'Internet Explorer 5.01' Patches - 50% - 1 out of 2 patches installed
Missing 'SQL Server 2000' Patches - 50% - 3 out of 6 patches installed
Missing 'Windows 2000 Server' Patches - 33% - 4 out of 6 patches installed
Missing 'Windows Media Player 6.4 for Windows 2000' Patches - 0% - 5 out of 5 patches installed
ECORAQA\BUNNYEARS IP Address: ; Operating System: Windows NT Workstation 4.0
Missing 'Internet Explorer 6' Patches - 16% - 5 out of 6 patches installed
Missing 'Microsoft SQL Server 2000 Desktop Engine (MSDE 2000)' Patches - 100% - 0 out of 1 patches installed
Missing 'SQL Server 2000' Patches - 50% - 3 out of 6 patches installed
Missing 'Windows Media Player 6.4 for Windows NT 4.0' Patches - 20% - 4 out of 5 patches installed
Missing 'Windows NT Workstation 4.0' Patches - 67% - 22 out of 68 patches installed
ECORAQA\DAYTON IP Address: ; Operating System: Windows XP Professional
Missing 'Internet Explorer 6' Patches - 0% - 5 out of 5 patches installed
Missing 'Windows Media Player for Windows XP' Patches - 0% - 3 out of 3 patches installed
Missing 'Windows XP Professional' Patches - 0% - 21 out of 21 patches installed
ECORAQA\DAYTON IP Address: ; Operating System: Windows XP Professional
Missing 'Internet Explorer 6' Patches - 0% - 12 out of 12 patches installed
Missing 'Microsoft SQL Server 2000 Desktop Engine (MSDE 2000)' Patches - 100% - 0 out of 2 patches installed
Missing 'Windows Media Player for Windows XP' Patches - 0% - 6 out of 6 patches installed
Missing 'Windows XP Professional' Patches - 8% - 42 out of 46 patches installed
Done
Local intranet

6. Click **Go**.
7. Browse the resulting report.

Tips:
Options left blank or not selected return ALL (vs none) by default.
An asterisk (*) functions as a wildcard in a search - returning ANY character as a match.
The **About** link provides version information.
The two **Export Report...** links save the report to DOC or CSV format.

The online Reporting Center performance varies based on how recently the Microsoft .NET pages have been compiled and / or restarted. The Microsoft .Net Framework documentation includes information about optimizing the machine.config file.

Administering the Reporting Center

Reporting Center Settings

1. The first time you access the Reporting Center (or by choosing **Administration... Settings...** in the left pane), you may be prompted for **Settings** to configure the Reporting Center.
2. Specify the Server Name (for SQL - server name or server, backlash, instance name; for MSDE - instance name).

   Tip: The SQL instance name is, by default, the server name, then, for additional instances, the server name appended with backslash and the named instance name. *Please consult the SQL Books Online installed optionally with the SQL server install for more details about naming conventions, named instances, and multiple instances.*
3. Specify the Database Name (by default, EcoraPatchDB) to which to connect and that you want to query (configured in setup and available in **File... Settings...** on the **Database** tab (in case you've forgotten the exact name).
4. Select the authentication method; either **Trusted connection** or **SQL Authentication**.
5. If you select SQL authentication, enter your login and your password.
6. Enter the mail server the Reporting Center should utilize.
7. Enter an email address from which reports will be sent.
8. Click **Submit** to save these settings (or **Close** to cancel).

Administering Users

1. Choose **Administration... Users...** in the left pane.

2. Select the domain from which to select users.
3. Select any users you wish to add by checking the box to their left.
4. Click **Add**.

Troubleshooting

Please refer to the online help system for troubleshooting information on the following:

Connecting & Scanning
Analysis - Under the Hood
Patch Repositories
Push Patch / Installation
Service Packs
Microsoft Patches
SQL Patches
Log Files
Reporting Center
Optional Agent
Migrating from Patch Manager 3.x
Port Usage
Command Line Operation
Limiting DB Memory Usage

The online help system includes appendices containing specialized information, such as command line operation and port usage for Patch manager communication.

Tip: The Support area of Ecora's website (http://www.ecora.com/ecora/support/) includes links to the system requirements, start-up guides, evaluation guides, helpful tools and utilities, and the FAQs (Frequently Asked Questions) page includes information about common questions and answers you might find helpful.

Ecora Copyright Notice

Copyright © 1999 - 2005 Ecora Software Corporation. All rights reserved.

Ecora, Patch Manager, PatchLite, PatchMeister, PatchMeister Pro, Enterprise Auditor, Configuration Reporter, Configuration Auditor, ecora.com, Ecora Application Server, My-ecora, and the names of any Ecora products referenced herein are either trademarks and/or service marks or registered trademarks of Ecora Corporation.

Microsoft, Windows, Windows NT, Windows XP, Windows Workstation, IIS, SQL Server, Visio, and BackOffice are either trademarks or registered trademarks of Microsoft Corporation.

Solaris is a registered trademark of Sun Microsystems, Inc.

Other product, operating system, and company names mentioned herein may be trademarks and/or service marks of their respective owners.

SUN, Sun OS, Solaris, and NFS are (registered) trademarks of Sun Microsystems, Inc.
SPARC is a registered trademark of SPARC International, Inc. Products bearing the SPARC trademarks are based on an architecture developed by Sun Microsystems, Inc.
HP-UX is a trademark of Hewlett-Packard Company.
AIX is a trademark of International Business Machines Corporation.
UNIX is registered trademark of AT&T, with versions licensed exclusively through X/Open Company Limited and/or The Open Group.
Linux is a registered trademark of Linus Torvalds.
Motif and UNIX are registered Copyright© 2000 by Red Hat, Inc.

Ecora software uses PuTTY code for SSH connections. Please see the PuTTY license for details.